# Chapter 2 LEARNER BOOKLET Risk and Risk Management

*Note:*



***Please note due to the ever changing operating environment for Financial advisers, rates and figures provided in the course work are subject to change some every quarter, therefore it is imperative that you complete your own research so that you are familiar with the current rates or figures which may not necessarily be reflected in the coursework at the time of you undertaking your studies.***

Site: IIT eLearning Platform
Course: Principles of Finance and Mortgage Broking Management (New) (DIPLOMA)
Book: Chapter 2 LEARNER BOOKLET Risk and Risk Management
Printed by: Arie Boles
Date: Monday, 21 August 2023, 5:24 PM

# Table of contents

# 1. Section Outline

Unless a business is regulated by APRA, ASIC-approved ACL licensed mortgage brokers must have measures in place to ensure compliance with their obligation to have adequate risk management systems implemented on an ongoing basis. *The National Consumer Credit Protection (National Credit Act) Act 2009* requires that mortgage brokers are expected to have a structured and systematic process for identifying, evaluating and managing risks faced by the business. Refer RG 205.73–RG 205.78 for further information.

ASIC also expects risk management systems to specifically address the risk that a business's financial resources will not be adequate to ensure they are able to carry on the business in compliance with their credit licence obligations or to wind up the business in an orderly manner. Refer RG 207.8–RG 207.11 for further information.

This topic introduces and explains the concepts of risk and risk assessment within an enterprise risk management framework (ERM) that will support Finance/Mortgage Brokers at organisational and agency level.

**Learning Outcomes**

After completing this section you should be able to:

- Identify and describe risk.
- Identify and assess controls.
- Develop risk evaluation criteria.
- Assess current exposure.
- Compare exposure with guidelines.
- Communicate with relevant internal and external stakeholders at each stage.

***Please note due to the ever changing operating environment for Financial advisers, rates and figures provided in the course work are subject to change some every quarter, therefore it is imperative that you complete your own research so that you are familiar with the current rates or figures which may not necessarily be reflected in the coursework at the time of you undertaking your studies.***

# 2. Introduction

Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

Risks can come from uncertainty in financial markets, project failures, legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attacks from an adversary. Several risk management standards have been developed including the Project Management Institute, the National Institute of Science and Technology, actuarial societies, and ISO standards.

Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety.

Enterprise risk management (ERM) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization’s objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, organisations or agencies protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

# 3. Communication and Consultation

As with any planning, project management and decision-making process, communication and consultation play an important role in all stages of the risk management process. The effective management of risk and identification of business opportunities cannot be achieved without ensuring all parties with a vested interest, including both internal and external stakeholders, are consulted. The effectiveness of the Risk Management process depends upon, amongst other things, involving the right people at the right time.

Communication is the sharing of information and viewpoints. Effective communication has the following attributes:

· It is multi-directional. Information, ideas and perspectives are shared across functional areas, and senior management are receptive to the views of their subordinates.

· It involves information and opinions. Other people's perspectives are understood and acknowledged. Factual information is gathered from all relevant sources. No individual or department has a monopoly on 'the facts'.

· It is interactive. Listening is as important as talking. Good communication involves the sharing of information, opinions and experiences.

· It is respectful. It focuses on ideas and information, not personalities. Communication is most effective in an environment where people are valued and their viewpoints are respected.

· It engages the participants, promoting their understanding and ownership of the outcomes.

Consultation is a process that uses communication to make effective decisions. Importantly, consultation is not an outcome or an end in itself; it is a means by which outcomes are achieved. Consultation gives stakeholders the opportunity to influence decisions, however, it is not joint decision-making, but rather an effective way to receive useful input and ensure that all relevant viewpoints are taken into account in identifying and evaluating risks.

Communication and consultation are essential to the overall risk management process as well as each individual step in that process.

A well-structured approach to communication and consultation can provide the following benefits:

· Organisational coherence and a positive culture for risk management implementation

· Trust and understanding, resulting in better internal and external relationships

· The risk management process becomes tangible: people know what it is and how it works

· Integration of multiple perspectives

· Risk management embedded as an on-going part of management and organisational practice

Each step of the Risk Management process relies on communication and consultation to achieve its purpose. For instance, in setting the context, consultation with internal and external stakeholders is essential to reach a thorough understanding of the operating environment and to define the purpose and scope of the exercise. In risk identification, a diversity of input can prevent important risks being overlooked and ensure that risks are accurately described. In the risk assessment process, communication and consultation allows all perspectives to be considered in arriving at a realistic level of risk. Risk treatment is more effective because treatment plans are better understood and the monitor and review process depends upon effective communication to ensure risk information is in use and current.

Communication and consultation does not mean asking everybody their opinion about everything. When developing a strategy to implement a formal risk management processes within your organisation or agency, you may wish to consider the following in relation to communication and consultation requirements:

· *Objectives* – What are the specific aims and goals of involving different parties in the process?

· *Participants* – Who are the appropriate parties to be involved at each step of the process?

· *Perspectives* – What particular contribution or viewpoint is anticipated and required from each participant?

· *Methods* – How will consultation take place? It may not always be practical to get all the parties together in one place.

Such consultation ensures that any differences of opinion or different perceptions of the risk are considered, understood and addressed. Similarly it provides two-way communication to identify opportunities towards business improvement. In summary, management has a responsibility to ensure that all relevant stakeholders are identified and consulted as part of the risk management process.

# 4. What is Risk?

Risk takes many forms because it is part of every human endeavour. You take risk every time you act: from crossing the street, to buying a stock, to driving a car, to getting on an aeroplane, to drinking a glass of pasteurized milk. We are exposed to risks of different degrees. While some of these risks can be reduced through a number of avenues, some of them can simply be accepted whilst others can be planned for. Risk is incorporated into so many different disciplines from insurance to engineering to portfolio theory that it should come as no surprise that it is defined in different ways by each one. Generally when people talk about risk, they focus on financial risk.

Risks can be categorised as 'pure' or 'speculative'. **Pure risk** describes a situation where two options are possible: either a negative event will occur, or it won't (e.g. a house will suffer damage that falls within its insurance policy, or it won't). In the case of **speculative risk**, three options are possible – negative, neutral or positive. In addition to a 'bad' event occurring, or not occurring, there is also the possibility of a positive event occurring, representing a gain of some sort. **Positive risks** are uncertainties that could bring *additional benefits* if they were to occur. A risk or gamble with a positive impact is an *opportunity*, whereas a risk with negative impacts is a *threat.*

Similar elements of risk are sometimes referred to as **risk clusters**, as they describe groupings of types of risk. These can vary from business to business but there are some risks most businesses or agencies have in common.

A risk cluster might consist of groupings like the following, some of which are described below:

- compliance risks
- employee risks
- environmental risks
- financial risks
- operational risks
- political and economic risks
- strategic risks
- business risks
- legal risks
- physical risks

As well as listing the risks, it's also useful to list what the consequences could be if the risks actually happen.

### Compliance Risks

Compliance risks are part of the laws and regulations a business must meet, such as taxation, employment, health and safety, and fair trading. Some potential risks are:

- Regulations might increase production costs, e.g., higher quality standards, changes and implication of laws, regulations, and rules
- Health and safety changes could add to costs, e.g., having to provide safety equipment to the workers

*Possible consequences*: fines or legal problems.

### Employee Risks

Although employees are vital to business success, there are risks associated with having employees. Some risks are:

- key staff being ill and unable to work at an important or extended time
- industry strike action

*Possible consequences*: customer service suffers, disruption to production.

### Environmental Risks

Each location and its business practices will influence the likelihood of each risk, but some to consider are:

- natural disasters such as bush fire, hail, flooding and wind storms
- property damage such as water pipes bursting or power failure

*Possible consequences*: loss or damage to stock or building, disruption.

### Financial Risks

Financial risks are part of the financial structure of a business, business transactions, and the financial systems used. Some possible risks to consider are:

- being overly reliant on a single customer
- changes in interest rates

*Possible consequences*: entire operation stops after main customer stops ordering from business, cash flow shortage.

### Health and Safety Risks

Apart from the legal and moral reasons for keeping a business or agency safe for employees, customers and others, a business could suffer if it does not manage the health and safety risks.

*Possible consequences:* business could be sued, get a bad reputation or be heavily fined. WorkSafe Injury Insurance premiums would also increase.

### Operational Risks

These are part of a business' operational and administrative procedures. These include:

- disorganised or inaccurate record keeping
- outdated or faulty IT systems
- interruptions to the supply chain

Each operation's potential risks need to be looked at, preferably independently, and then prioritised. For instance, would a truck drivers' strike stopping deliveries be more damaging than forgetting to send a monthly statement?

*Possible consequences*: customers see business as unreliable, IT system causes loss of all data.

**Political and Economic Risks**

Some businesses can be affected by a change of government and government policy. Likewise, economic changes, such as a recession or interest rate fluctuations, could be a risk to a business.

The risks are not always direct – an economic slump may stop consumers buying from the business, or simply buying far less. The reverse is also true, e.g., sudden increased demand.

**Strategic Risks**

These affect particular industries. They include the effects of:

- changes in customer demand
- new technology or practices

*Possible consequences*: the market sees the business product or service as outdated, or competitors offer a much lower price or better quality.

# 5. Risk Management

As the Internet has come of age, companies have been rethinking their business models, core strategies, and target customer bases. ‘Getting wired’, provides businesses with new opportunities, but brings new risks and uncertainty into the equation.

Mismanagement of risk can carry an enormous cost. In recent years, business has experienced numerous, related risk reversals that have resulted in considerable financial loss, decrease in shareholder value, damage to company reputations, dismissals of senior management, and, in some cases, the very dissolution of the business. This increasingly risky environment, in which risk mismanagement can have dire consequences, mandates that management adopt a new more pro-active perspective on risk management (Cowherd & Manson, 2004). Therefore, the importance of risk management cannot be over-stated.

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

· providing a framework for an organisation or agency that enables future activity to take place in a consistent and controlled manner;

· improving decision-making, planning and prioritisation by comprehensive and structured understanding of business activity, volatility and project opportunity/threat;

· contributing to more efficient use/allocation of capital and resources within the organisation or agency;

· reducing volatility in the non-essential areas of the business;

· protecting and enhancing assets and company image;

· developing and supporting people and the organisation’s knowledge base, and

· optimising operational efficiency.

Notwithstanding the inherent benefits of a Risk Management structure, within the *National Consumer Credit Protection Act (2009)*, ACL licensed mortgage brokers must ‘have adequate risk management systems’ in place (Section 47(1)(l)(ii)). (Refer also National Consumer Credit Protection Regulations 2010 Subsection 47(1)(h)(ii).)

**What is Risk Management?**

Risk management is a process used to avoid, reduce or control risks. Some risks can be insured against, others cannot. Thus, Risk Management is simply the practice of systematically identifying and understanding risks and the controls that are in place to manage them.

Ultimately, the process gets you to a point of deciding whether, in the context of a particular strategy, activity or function, a risk is acceptable or requires further action. That context might also include:

· any related projects or organisations

· any resources, including physical assets, which are vital to operations

· key operational elements and service of the organization

· how an organisation or project is organised and its capabilities

· own role and responsibilities in relation to overall project or organisation design

Enterprise risk management (ERM) is a relatively new discipline that focuses on identifying, analysing, monitoring, and controlling all major risk classes (e.g., credit, market, liquidity, operational risk classes). Operational risk management (ORM) is a subset of ERM that focuses on identifying, analysing, monitoring, and controlling operational risk.

The primary reason for managing risk is to enable business to successfully achieve their goals. With the growing need for transparent decision-making, a structured, systematic risk management process demonstrates the due diligence that is required and provides an audit trail for decision making. A comprehensive understanding of the risk exposures facing a business also facilitates effective planning and resource allocation, and encourages a pro-active management culture, with flow-on benefits for every aspect of a business’s or agency’s operation.

**Exposure**

When assessing risk, **exposure** to risk is based on **consequences** and **likelihood**. If the consequences of an event or a planned action are minimal, then the risk is not considered great, similarly if a risk is highly unlikely to occur, it weighs much more lightly than if it is likely and imminent. Solutions or **mitigation** of risks might be possible using technological, human and organizational resources to reduce the probability or the severity of adverse events. Income protection insurance would for instance mitigate or remove the risk of default in loan repayments. Other ways of dealing with risk are by **avoiding** it altogether, by not taking on the risk in the first place – the man who does not gamble has no risk of losing his money in that manner. **Tolerating** a risk is another means of dealing with it – effectively taking the chance that the risk will not occur at all or assessing that (as mentioned above) the consequences or likelihood of the risk are not too great. Another way to limit exposure is to **transfer** the risk to another party. When a loan is given without security, it is often done by requiring the borrower supply a guarantor who will take on the risk of non-payment. Effectively the risk is transferred, for someone else to have to deal with.

Ignoring the risks which apply to a business’s activities or the events planned, could impact on the following:

· the health and safety of employees, customers, volunteers and participants

· organisation’s reputation, credibility and status

· public and customer confidence in the organisation or agency

· organisation’s financial position

· plant, equipment and the environment.

The global financial crisis in 2008 demonstrated the importance of adequate risk management. As a result, a systematic approach to managing risk is now regarded as good management practice.

**Types of Risk Management**

There are different types of risk management and the characteristics and procedures of each type are different from the other.

Commercial enterprises apply various forms of risk management procedures to handle different risks because they face a variety of risks while carrying out their business operations.

All these risk management processes play a significant role behind the growth of an organization in the long term. Effective handling of risk ensures the successful growth of an organization.

In the Financial Services industry, various types of risk management can be categorized into the following:

· *Operational Risk Management:* Operational risk management deals with technical failures and human errors.

· *Financial Risk Management:* Financial risk management handles non-payment of clients and increased rate of interest.

· *Market Risk Management:* Deals with different types of market risk, such as interest rate risk, equity risk, commodity risk, and currency risk.

· *Credit Risk Management:* Deals with the risk related to the probability of non-payment from the debtors.

· *Quantitative Risk Management:* In quantitative risk management, an effort is carried out to numerically ascertain the possibilities of the different adverse financial circumstances to handle the degree of loss that might occur from those circumstances.

· *Commodity Risk Management:* Handles different types of commodity risks, such as price risk, political risk, quantity risk and cost risk.

· *Bank Risk Management:* Deals with the handling of different types of risks faced by the banks, for example, market risk, credit risk, liquidity risk, legal risk, operational risk and reputational risk.

· *Non-profit Risk Management:* This is a process where risk management companies offer risk management services on a non-profit seeking basis.

· *Currency Risk Management:* Deals with changes in currency prices.

· *Enterprise Risk Management:* Handles the risks faced by enterprises in accomplishing their goals.

· *Project Risk Management:* Deals with particular risks associated with the undertaking of a project.

· *Integrated Risk Management:* Integrated risk management refers to integrating risk data into the strategic decision making of a company and taking decisions, which take into account the set risk tolerance degrees of a department. In other words, it is the supervision of market, credit, and liquidity risk at the same time or on a simultaneous basis.

· *Technology Risk Management:* It is the process of managing the risks associated with implementation of new technology.

· *Software Risk Management:* Deals with different types of risks associated with implementation of new software.

**Risk Management Standard**

After five years of development, the Joint Technical Committee on Risk Management approved the adoption of ISO 31000 as 'AS/NZS ISO 31000:2009 Risk Management — Principles and Guidelines'[1], making the previous Standards Australia AS/NZS 4360:2004 (on which the standard was based) redundant.

Whereas the Standards Australia approach provided a process by which risk management could be undertaken, the purpose of ISO 31000:2009 is applicable and adaptable for 'any public, private or community enterprise, association, group or individual.[2]' Accordingly, the general scope of ISO 31000 – as a family of risk management standards – is not developed for a particular industry group, management system or subject matter field in mind, rather to provide best practice structure and guidance to the entire management system that supports the design, implementation, maintenance and improvement of risk management processes.

In 2009, the International Standards Organization published ISO 31000, the new standard for Risk Management, noting that:

*"To be successful, risk management should function within a risk management framework which provides the foundations and organizational arrangements that will embed it throughout the organization at all levels. … The framework should ensure that risk information derived from these processes is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels."*

Australian Standard's AS/NZS ISO 31000:2009 sets a common approach and responsibilities for all staff to systematically manage risk consistent with this Australian standard on risk management.

**Definition of Risk**

Risk is incorporated into so many different disciplines from insurance to engineering to portfolio theory that it should come as no surprise that it is defined in different ways by each one. A risk was defined by the Australia/New Zealand Standard for Risk Management (AS/NZS 4360:2004) as: *"… the possibility of something happening that impacts on your objectives. It is the chance to either make a gain or a loss. It is measured in terms of likelihood and consequence."*

Whilst the previously standard focused on risk as being the chance of something happening that will have an impact on objectives, the new definition set out in ISO Guide 73 is that risk is:

*"[The] effect of uncertainty on objectives".*

In order to assist with the application of this definition, Guide 73 states that an effect may be positive, negative or a deviation from the expected, and that risk is often described by an event, a change in circumstances or a consequence. This definition links risks to objectives. Therefore, this definition of risk can most easily be applied when the objectives of the organisation or agency are comprehensive and fully stated. Even when fully stated, the objectives themselves need to be challenged and the assumptions on which they are based should be tested, as part of the risk management process

**Nature and Impact of Risk**

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

**Illustrated Example 1**

*Consider the infrastructure of an organisation or agency and the implementation of a new IT system.*

The choice of hardware and software are strategic decisions. If these choices are incorrect, the consequences will not be obvious for some time. The associated risks are strategic risks and these risks will be taken with the intention of achieving benefits. Correct strategic decisions deliver benefits that result in achievement of the upside of risk.

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

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

For example, looking at a part of an operation that provides a consulting service, one could identify a risk as follows in Table 1:

**Table 1: Nature and Impact of Risk**

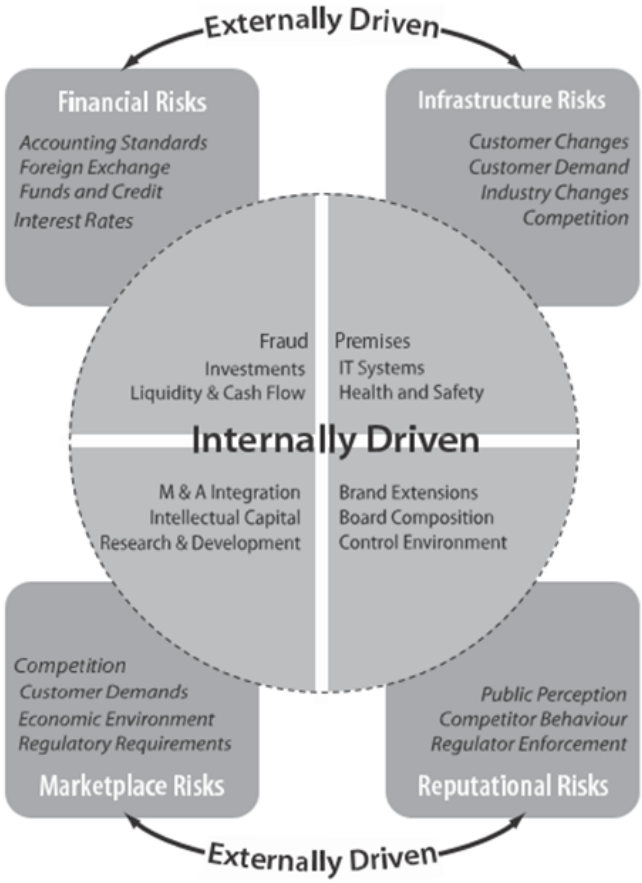
| Key Activities | Critical Success Factors | Risks |
|---|---|---|
| Providing advice to clients | Accuracy of information | Incomplete or inaccurate information provided to clients. |

For each risk, you should identify possible causes of the risk event. Each risk may have one or more causal factors which can either directly or indirectly contribute to the risk event occurring. Identifying the range of causes will help you to better understand the risk, evaluate the adequacy of existing controls and design effective risk treatments.

### External and Internal Risk Drivers

The risks facing an organisation or agency and its operations can result from factors both external and internal to the organisation or agency. The following diagram summarises examples of key risks in these areas and shows that some specific risks can have both external and internal drivers and therefore overlap the two areas. They can be categorised further into types of risk such as financial, infrastructure, marketplace, reputational, etcetera.

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




[1] http://infostore.saiglobal.com/store/Details.aspx?productID=1378670

[2] http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170

# 6. Risk Management Process

The risk management process can be presented as a list of co-ordinated activities. There are alternative descriptions of this process, but the components listed below are usually present.

This list represents the 7Rs and 4Ts of (hazard) risk management:

· recognition or identification of risks

· ranking or evaluation of risks

· responding to significant risks

o tolerate

o treat

o transfer

o terminate

· resourcing controls

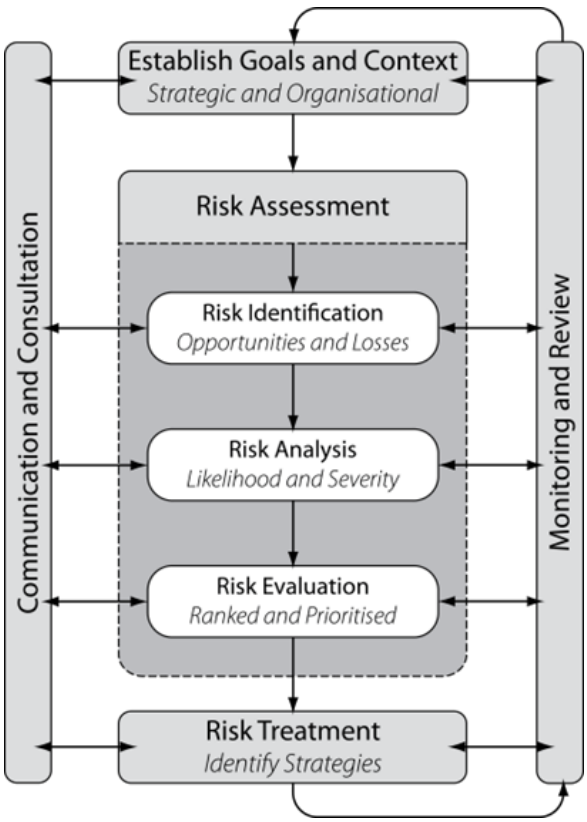
· reaction planning

· reporting and monitoring risk performance

· reviewing the risk management framework

Risks can sometimes be managed or mitigated in a manner which minimises adverse outcomes while still maintaining the maximum delivery of benefits. To do so requires that various mitigation measures for specific risks be identified and evaluated as outlined in the following graphic.

These generic processes as outlined in the graphic below provide a structured framework for managing strategic, operational and project management risks across a department, portfolio and whole-of- organisation or agency levels.




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

Risk management is to be applied at all stages in the life of an activity, function, project or asset. The maximum benefit is usually obtained by integrating and applying the risk management process from the beginning to the management of potential gains/losses.

**Illustrated example 2**

*Dealing with the Risks of Cloud Computing*

As we emerge from the economic downturn, more and more companies are considering “cloud computing” solutions as a way to keep information technology costs in control. However, some companies are fearful of the unknown aspects of managing information within the cloud. These fears may be justified, but they can certainly be alleviated by conducting a thorough risk assessment and vendor due diligence exercise prior to venturing into the cloud.

It all starts with what the company is looking to achieve through cloud computing and whether the investment is worth the risk. For example, will the application hosted in the cloud be customer facing and subject to strict regulatory standards? If so, then the risk assessment should include the probability and impact of events such as a data breach or unplanned downtime.

Once the risk assessment has been completed and the investment decision has been made, then a comprehensive due diligence exercise should be conducted. Some vendors may suggest simply relying on their SAS 70 report from their external auditing firm rather than performing a due diligence exercise. While SAS 70 reports are useful, they are not specific to the relationship between the two companies. It is imperative that the following areas are examined in relation to a company’s current information security policies and overall operating expectations.

1) Organizational and Human Resource Security

2) Access Control
3) Asset Management
4) Physical and Environmental Security
5) Operations and Change Management
6) Disaster Recovery and Business Continuity
7) Privacy
8) Regulatory Compliance

Like any other partnership or outsourcing agreement, the time to address potential risks and issues with cloud computing is at the very beginning of the relationship. By doing so, both the company and the vendor will benefit from the opportunity to understand each other's expectations. It will also serve as the foundation for a successful cloud computing solution.

**Establish Goals and Context**

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

Risk management is considered in the context of the organisation's or agency's external and internal environments, the objectives and business relationships. This enables timely identification of emerging risk both at, and beyond, the departmental level to achieve business objectives.

To identify key risk areas, an organisation or agency conducts an environmental scan. The scan sets a strategic direction for risk management which can be amended, as more information comes to light, or as the organisation's or agency's capacity to manage risk increases.

Key questions to undertake in the scan include:

· *Risk type* – technological, financial, health, safety, etc.;
· *Risk source* – external (political/economic/natural disaster) or internal (reputation; security, knowledge management, etc.);
· *What is at risk* – area of impact and the type of exposure (people, reputation, program results, assets, etc.), and
· *The level of control* – degree the department can influence/affect or manage risk.

**Departmental Categories of Risk Criteria**

The context is used to develop the following broad categories of risk criteria for a department or agency to evaluate risk:

· Workplace Health and Safety;
· Integrity and Reputation;
· Natural Environment;
· Finance;
· Legal and Contractual;
· Information, Communications and Technology;
· Operations; and
· Stakeholders

**Risk Evaluation**

An organisation must decide upon the **criteria** against which risks are to be **evaluated** – a means of measuring what is important to cultivate and protect from risk – prioritising as between increased profits and customer satisfaction for instance. Organisational processes and procedures weigh heavily, as an organisation's internal policies and priorities will dictate which sorts of risks are considered more severe and which demand most attention and management at any given time. Once relevant organisational guidelines are identified, risk exposure levels can then be compared with such guidelines. Priorities may be based on operational, technical, financial, legal, social, humanitarian or other criteria. The risk evaluation criteria may also be affected by internal and external perceptions and legal requirements.

**Stakeholders**

Stakeholders are those who have the possibility of gaining benefits or experiencing losses or harm as a result of company operations. Stakeholders can include a range of individuals, organisations and entities such as:

· Contractors
· Employees
· Financial Managers
· Insurance Agent
· Managers
· Public
· Service Providers
· Suppliers
· Consumers
· Unions
· Volunteers
· Mortgagees
· Mortgage Brokers

- Mortgage Managers
- Insurance and Finance Companies
- Aggregators
- General Lenders
- Industry Associations
- External Dispute Resolution Agencies
- Barristers and Solicitors
- Government Agencies
- Referrer Networks
- Policy Makers, etcetera

Stakeholders might be internal to the organisation, including its policy makers, or those providing services within, or receiving services from the organisation; or they might be external to the organisation, but having an interest in the function being assessed, like for instance suppliers, customers, regulators or shareholders. By being aware of the interrelationship between stakeholders and the organisation, risk can be better anticipated and managed. The risk for instance, of required goods being delivered on time can be better assessed and handled if communicating openly with the supplier of those goods.

It is generally considered good practice to engage with stakeholders, as opposed to ‘top-down’ management. Developing a two-way flow of communication in which the organisation listens to and makes a sincere attempt to respond to stakeholder concerns and inputs, helps in determining and establishing shared values and areas of mutual interest or common concern. Perhaps a simple example of stakeholder interests is in the situation where operational systems in a workplace are upgraded, causing changes to each employee’s day to day work practices. Consultation in such situations can help to define and address the concerns, difficulties or other issues arising for employees from such changes. Ultimately a smoother transition might then be negotiated by taking various stakeholders’ positions into account. This in turn might reduce other risks, perhaps associated with workloads lagging behind required deadlines during the transition period.

In each situation when risks or risk cluster elements are identified, these should be clearly communicated and described to relevant stakeholders, who are to be identified and their views sought and recorded. Information pertinent to financial risk identification is provided to stakeholders at each stage of assessing the organisation's exposure to risks.

Interaction with internal and external stakeholders ensures that all relevant risks and business improvement opportunities are addressed and there is a shared understanding. The two-way dialog with stakeholders brings insight into how the stakeholders will respond to new policies, projects or decisions, and allows stakeholders to understand why particular actions have been taken. (Refer RG 205.69)

Once the context for a particular risk assessment has been specified, and the particular strategy, activity or project defined, the next step is to identify the critical success factors (CSF) and key dependencies associated with it. A CSF is defined as any essential resource, expertise, input, or other factor, which is critical to the success of that particular strategy or activity. A key dependency is relationship with or reliance upon another person, section or organisation whose input is vital to a successful outcome. These success factors and dependencies become the basis to identify risk; anything that has a negative impact upon them constitutes a risk to the desired outcomes. Measures of success may include:

- Costs
- reductions in impact
- reductions in likelihood
- reductions in occurrence

### Risk Assessment

Risk assessment is a fundamentally important part of the risk management process. In order to achieve a comprehensive risk management approach, an organisation or agency needs to undertake suitable and sufficient risk assessments.

Risk Assessment is defined by the ISO/IEC Guide 73 as “the overall process of risk analysis and risk evaluation”, and will be required as part of the decision-making processes intended to exploit business opportunities. One way of ensuring that risk is part of business decision-making is to ensure that a risk assessment is attached to all strategy papers presented to Management. Likewise, risk assessment of all proposed projects should be undertaken and further risk assessments should be undertaken throughout the project. Finally, risk assessments are also required in relation to routine operations.

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

A range of the most common risk assessment techniques is set-out in Table 2:

**Table 2: Risk Assessment Techniques**

| Technique | Description |
|---|---|

| | |
|---|---|
| • Questionnaires and checklists | Use of structured questionnaires and checklists to collect information to assist with the recognition of the significant risks. |
| • Workshops and brainstorming | Collection and sharing of ideas and discussion of the events that could impact the objectives, stakeholder expectations or key dependencies. |
| • Inspections and audits | Physical inspections of premises and activities and audits of compliance with established systems and procedures. |
| • Flowcharts and dependency analysis | Analysis of processes and operations within the organisation to identify critical components that are key to success. |
| • HAZOP and FMEA approaches | Hazard and Operability studies and Failure Modes Effects Analysis are quantitative technical failure analysis techniques. |
| • SWOT and PESTLE analyses | Strengths Weaknesses Opportunities Threats (SWOT) and Political Economic Social Technological Legal Environmental (PESTLE) analyses offer structured approaches to risk recognition. |
| • Scenario analysis/thinking/planning | A strategic planning tool or method for improving decision-making against a background of possible future environments. |

**Risk Identification**

Risk identification should be approached in a methodical way to ensure that all significant activities within the organisation or agency have been identified and all the risks flowing from these activities defined. These can be:

· *Physical:* This could involve personal injuries, environmental and weather conditions and the physical assets of your organisation or agency. (Refer RG 205.30.)

· *Financial:* This could mean fraud, theft, membership fees, insurance costs, loss of funding, etc. (Refer RG 207.1, RG 207.9)

· *Legal:* This includes responsibilities imposed by federal, state or local governments. (Refer RG 205.)

· *Ethical or Moral:* Involving actual or potential harm to the reputation or beliefs of an individual or organisation.

All associated volatility related to these activities should be identified and categorised.

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

· *Strategic:* These concern the long-term strategic objectives of the organisation or agency. They can be affected by such areas as capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment.

· *Operational:* These concern the day-to-day issues that the organisation or agency is confronted with as it strives to deliver its strategic objectives.

· *Financial:* These concern the effective management and control of the finances of the organisation or agency and the effects of external factors such as availability of credit, foreign exchange rates, interest rate movement and other market exposures.

· *Knowledge Management:* These concern the effective management and control of the knowledge resources, the production, protection and communication thereof. External factors might include the unauthorised use or abuse of intellectual property, area power failures, and competitive technology. Internal factors might be system malfunction or loss of key staff.

· *Compliance:* These concern such issues as health & safety, environmental, trade descriptions, consumer protection, data protection, employment practices and regulatory issues. (Refer RG 205.52.)

For each risk, you should identify possible causes of the risk event. Each risk may have one or more causal factors which can either directly or indirectly contribute to the risk event occurring. Identifying the range of causes will help you to better understand the risk, evaluate the adequacy of existing controls and design effective risk treatments.

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

**Risk Analysis**

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

This step of the risk assessment process requires that for each risk, organizations **identify the current controls** and their **effectiveness in preventing** the risk from eventuating **or minimising** its impact should it occur.

**Controls** are the measures which limit the impact of risks, like for instance, the traffic controls that regulate vehicles. At a busy intersection, where collisions occur frequently, a need might be established for additional or improved controls, like, for instance, a roundabout, or lights, to be installed. If required, the need for such a change is reported, and appropriate controls can be recommended and then implemented, or existing ones amended. In this case, traffic lights might be introduced in order to regulate and direct the flow of vehicles, so that the risk or likelihood of a collision is reduced significantly.

In a financial setting, lenders have all manner of controls in place which limit risk when it can be predicted. Certain risk reduction controls are 'set in stone' in the policies and procedures of an organisation – like lending only to those who have some form of income – while other finer details may need to still be handled or updated from day to day, or week to week, like the risk of lending to a person employed by a company when it is learned that it is be soon to be placed under receivership. Any number of external factors can be in a constant state of flux, so the need is clear, to monitor and assess controls on an ongoing basis in light of changing circumstances or risks.

Various methods of identifying financial risks might be employed – like monitoring stock exchange reports, financial news and economic developments – or the basics, as in requiring an applicant to provide their financial information and valid identification in their finance application.

Once a control has been noted, its effectiveness can be assessed, such as:

I = Inadequate

A = Adequate

E = Excellent

It is important to remember that current controls not fully implemented will not be fully effective. The implementation of these controls may form the basis of cost-effective treatment strategies to address unacceptable risks. Note these controls for consideration when developing treatment strategies.

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

### Risk Estimation

The objective of risk analysis is to display the identified risks in a structured format, for example, by using a table. A risk description table can be used as an estimation tool to facilitate the description and assessment.

The likelihood and severity of risk can be estimated from the use of three forms of information and data collection processes, namely:

· *Qualitative:* Methods of analysis that use questioning and personal judgement to make a decision. These may include brainstorming, focus groups, expert or stakeholder input, questionnaires or intuition.

· *Semi-quantitative:* Methods that give quantitative ranking to a qualitative decision such as low-risk, medium-risk or high-risk.

· *Quantitative:* Methods that use research and/or measurement tools to make a decision. They may include probability and consequence analysis, modelling, statistical analysis, decision trees, event-tree analysis, etc.

For example, consequences both in terms of threats (downside risks) and opportunities

(upside risks) may be high, medium or low as identified in Table 3.

**Table 3: Consequences – Both Threats and Opportunities**

| | |
|---|---|
| High | · Financial impact on the organisation is likely to exceed $*x*.<br>· Significant impact on the organisation's strategy or operational activities.<br>· Significant stakeholder concern. |
| Medium | · Financial impact on the organisation likely to be between $*x* and $*y*.<br>· Moderate impact on the organisation's strategy or operational activities.<br>· Moderate stakeholder concern. |
| Low | · Financial impact on the organisation likely to be less than $*y*.<br>· Low impact on the organisation's strategy or operational activities.<br>· Low stakeholder concern. |

Probability may be high, medium or low but requires different definitions in respect of threats and opportunities of risks as shown in Table 4 and Table 5.

**Table 4: Probability of Risk Occurrence – Threats**

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

| Table 5: Probability of Risk Occurrence – Opportunities | | |
|---|---|---|
| Estimation | Description | Indicators |
| High (Probable) | Favourable outcome is likely to be achieved in one year or better than 75% chance of occurrence. | Clear opportunity which can be relied on with reasonable certainty, to be achieved in the short term based on current management processes. |
| Medium (Possible) | Reasonable prospects of favourable results in one year of 25% to 75% chance of occurrence. | Opportunities which may be achievable but which require careful management. Opportunities which may arise over and above the plan. |
| Low (Remote) | Some chance of favourable outcome in the medium term or less than 25% chance of occurrence. | Possible opportunity which has yet to be fully investigated by management. Opportunity for which the likelihood of success is low on the basis of management resources currently being applied. |

Many organisations find that assessing consequence and probability as high, medium or low is quite adequate for their needs and can be presented as a 3 × 3 matrix. Other organisations find that assessing consequence and probability using a 5 × 5 matrix gives them a better evaluation.

Identification of the risks associated with business activities and decision-making may be categorised as strategic, project/tactical, operational. It is important to incorporate risk management at the conceptual stage of projects as well as throughout the life of a specific project.

The use of a well-designed structure is necessary to ensure a comprehensive risk identification, description and assessment process. By considering the consequence and probability of each of the risks set-out Table 6, it should be possible to prioritise the key risks that need to be analysed in more detail.

| Table 6: Detailed Description Table | |
|---|---|
| 1. Name or title of Risk | · Unique identifier or risk index. |
| 2. Scope of Risk | · Qualitative description of the events, their size, type, number and dependencies. |
| 3. Nature of Risk | · Classification of risk, e.g., strategic, operational, financial, knowledge or compliance.<br>· Timescale of potential impact and description as hazard, opportunity or uncertainty. |
| 4. Stakeholders | · Stakeholders and their expectations. |
| 5. Risk evaluation | · Likelihood and magnitude of event and possible impact or consequences should the risk materialise at current level. |
| 6. Quantification of Risk | · Loss potential and financial impact of risk.<br>· Previous incidents and prior loss experience of events related to the risk. |
| 7. Risk Tolerance, Appetite or Attitude | · Significance and Probability.<br>· Value at risk.<br>· Probability and size of potential losses/gains.<br>· Objective(s) for control of the risk and desired level of Performance. |
| 8. Risk Response, Treatment & Control Mechanisms | · Primary means by which the risk is currently managed.<br>· Levels of confidence in existing control.<br>· Identification of protocols for monitoring and review. |
| 9. Potential Action for Improvement | · Recommendations to reduce risk.<br>· Potential for cost-effective risk improvement or modification.<br>· Recommendations and deadlines for implementation.<br>· Responsibility for implementing any improvements. |
| 10. Strategy and Policy Developments | · Responsibility for developing strategy related to the risk.<br>· Responsibility for auditing compliance with controls. |

### Risk Consequence Rating

A risk that eventuates may impact an organisation or agency across a number of different areas, to a greater or lesser extent. When analysing the consequences of a risk event, an organisation needs to consider the outcome or impact (Table 7) in relation to each of the consequence against the relevant category of criteria for a consistent approach to determine a level. For example, a risk may have an impact of 5 for Financial Loss and 4 for Reputation and Image and little or no impact in the other areas. Both ratings may be recorded, but the overall level of risk calculation is based on the highest value, which in this case is a 5.

Only select the Consequence Categories that are relevant to that risk. You do not have to rate every Consequence Category for each risk. Some consequences will not be applicable to a specific risk.

| Table 7: Risk Consequences | | | | |
|---|---|---|---|---|
| Level | Descriptor | Reputation | Financial | Operational Efficiency |
| 1 | Insignificant | Unsubstantiated<br>Low impact<br>Low profile | Negligible | Negligible |

| | | | | |
|---|---|---|---|---|
| 2 | Minor | Substantiated<br>Low impact<br>No management involvement | Low financial loss | May cause delay |
| 3 | Moderate | Substantiated<br>Low impact<br>Management involvement | Moderate financial loss | Major delay in deliverables |
| 4 | Major | Substantiated<br>High impact<br>Third-party involvement | Major financial loss | Failure of achievement or provision of deliverable |
| 5 | Catastrophic | Substantiated<br>Public embarrassment<br>Very high multiple impacts<br>High profile<br>Third-party actions | Extreme financial loss | Non-achievement of major key objectives |

**Table 8: Risk Assessment Criteria Table**

| Consequence | Likelihood | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| | Rare | Unlikely | Moderate | Likely | Almost Certain |
| 1 Insignificant | 1 | 2 | 3 | 4 | 5 |
| 2 Minor | 2 | 4 | 6 | 8 | 10 |
| 3 Moderate | 3 | 6 | 9 | 12 | 15 |
| 4 Major | 4 | 8 | 12 | 16 | 20 |
| 5 Catastrophic | 5 | 10 | 15 | 20 | 25 |
| | | | | | |
| Approved as at: | / /20 | | | | |
| By: | | | | | |
| Title: | | | | | |

To achieve an overall risk rating, the consequence rating is multiplied by the likelihood rating. The numerical level of risk is then aligned to a ranking key such as the example presented in Table 9.

**Table 9: Risk Acceptance Criteria Table**

| Level of Risk | Criteria for Management of Risk | | Responsibility |
|---|---|---|---|
| 1–3 | Acceptable | With adequate controls | Routine procedures |
| 4–5 | Monitor | With adequate controls | Operational Manager |
| 6–9 | Management Control Required | With adequate controls | Operational Manager |
| 10–14 | Urgent Management Attention | Only acceptable with excellent controls | Chief Executive Officer |
| 15–25 | Unacceptable | Only acceptable with excellent controls | Licensee/Stakeholder |

**Risk Evaluation**

Once the Level of Risk has been determined, the next step is to evaluate the risk and see where the risk fits against the organisation's or agency's overall risk criteria. An example (Table 9) is shown below. The table gives guidance as to the acceptability of the risk and the level of sign-off required.

Each risk that is identified needs to be allocated a Risk Owner. This is the person responsible for managing the risk, and is usually the person who is directly responsible for the strategy, activity or function that relates to the risk. Some of the key responsibilities of the Risk Owner include:

- Sign-off on acceptance of the risk
- Responsible for the regular review of the risk
- Responsible for the regular reporting on the risk
- Monitoring of controls
- Implementation of any risk treatments

Assigning risk ownership ensures a specific person is responsible and accountable for a particular risk. It is usually impractical and ineffective for risk ownership to be assigned to a body, such as a business unit or committee.

Once a risk has been analysed and evaluated, the Risk Owner makes an informed decision to do one of the following:

- *Retain the risk:* The reward outweighs the risk and the existing controls meet the criteria specified in the Risk Acceptance Criteria Table.
- *Avoid the risk:* Do not carry on with the activity that is associated with the risk or choosing another way to achieve the same outcome.
- *Treat the risk:* Reduce either the likelihood, consequence or both by improving existing controls or adding new controls, so that the risk can be accepted.
- *Transfer the risk:* Shift all or part of the responsibility of the risk to another party who is best able to control it.

The risk decision balances the issues of risk and reward. Should an opportunity be passed over because of the risks associated with it? Should more be done to manage the risk so as not to miss- out on the opportunity? These are questions that the organisation or agency will need to addresses. An organisation or agency cannot progress or improve without capitalising on opportunities, and opportunities will always have associated risks.

### Risk Likelihood

This describes how likely it is that a risk will eventuate with the defined consequences. Likelihood can be defined in terms of probability or frequency, depending on what is most convenient for the organisation's or agency's purposes. The likelihood that an event will occur is not always easy to assess. Subjective biases may give rise to different assessments by different people. To avoid this situation, and in order to provide a degree of consistency across an organisation or agency in assessing likelihood, Table 10 could be used as a guide.

When you are rating the likelihood of a risk, ask yourself "How likely (Likelihood Rating) is it for this risk (Risk) to occur, given the existing controls (Controls), to this extent or with this type and level of impact (Consequence Category/Rating)?"

**Table 10: Qualitative Measures of Risk Likelihood**

| Level | Descriptor | Detail Description | Frequency |
|---|---|---|---|
| 1 | Rare | This event may occur, but only in exceptional circumstances. | Less than once in 10 years. |
| 2 | Unlikely | This event could occur in some circumstances. | At least one in 10 years. |
| 3 | Possible | This event should occur in some circumstances. | At least once in 5 years. |
| 4 | Likely | This event will probably occur in most circumstances. | At least once per year. |

A risk map is a data visualization tool for communicating specific **risks** an organization faces. The goal of a **risk map** is to improve an organization's understanding of its **risk** profile and appetite, clarify thinking on the nature and impact of **risks**, and improve the organization's **risk** assessment model.

# 7. Risk Treatment

On completion of the risk assessment process, a risk management plan is to be developed. The plan will prioritise the risks that require treatment, identify the treatments that require implementation, and identify who is responsible for implementing particular treatments. Where appropriate, the plan should also identify critical implementation milestones and how these will be measured.

When determining the most appropriate treatment options, all risks need to be considered and their priority levels compared to each other. The resources available to treat these risks also need to be determined. The aim is to effectively identify and prioritise risks and to treat risks according to their priority in the most effective manner with the resources available. A further important consideration is the balancing of cost associated with the control against the benefit derived from it. In general, the cost incurred in managing risks needs to be commensurate with the benefits gained. There are four treatment options for managing risk listed as:

Avoid the activity that caused the risk: Regardless of the risks, some activities have to proceed. This means that a risk management plan of action must be formulated that ensures a reduction or elimination of the risks associated with these activities.

Accept or retain the risk: Some risks are worth taking and need to be retained. It is important to determine whether the head office, agency or department is in a position, either legally or financially to carry the risks. Resource requirements feature heavily in this strategy.

Reduce the likelihood of an occurrence or its consequences: Some actions that can be taken to reduce the likelihood or consequence of a risk include:

- regular audits and reviews;
- supervision and training;
- adequate controls and processes in place, and
- management of key relationships.

Insure or transfer the risk: The final treatment relates to the transfer of the risk to another party and/or coverage by an insurance facility. This choice will be driven by the evaluation of the risk versus the benefit of implementing the option.

In the previous step, risks were assessed and decisions were made to accept them or not. In practical terms, risk avoidance, i.e., ceasing the activity that creates the risk, is rarely a practical option. Agencies normally have their activities defined by a higher authority and if there are risks associated with those activities, a way must be found to manage them.

In some cases, existing controls will be deemed to be adequate and effective, and the risk will be accepted as it stands. In other instances, the risk will need to be more effectively managed before it can be accepted. This latter case requires the formulation of risk treatments. Risk treatment involves identifying a range of options to reduce the consequences and/or likelihood of a risk, or improve the controls rating, evaluating those options, preparing treatment plans, and implementing them.

**Identify, Evaluate and Select Treatment Options**

Each unacceptable risk will have a number of treatments. Other than the option of avoiding the risk entirely, treatment options will do one or all of the following:

- Reduce the likelihood of the risk eventuating
- Reduce the consequences of the risk if it eventuates
- Improve the controls rating to “Adequate” or “Excellent”

It is not always possible or cost-effective to treat all risks associated with a particular service or activity. For example, many government agencies are suppliers of last resort, and therefore some risks categorised as unacceptable may have to be accepted as long as the agency is doing all that is reasonable to control the risks. This situation places increased importance on controls assurance and the monitor and review process.

Managing risk is about doing all things reasonable, not all things possible. To evaluate the treatment options a number of selection criteria can be applied:

- *How will the treatment impact the Level of Risk?* – For each treatment option, a predicted level of risk should be calculated considering the impact of adding this option as a new control. Treatment options, which reduce the level of risk to an acceptable level, should be considered.
- *Cost of implementation versus benefits derived?* – Selecting appropriate options involves balancing the cost against the benefits derived. An option may appear to be the best option from a risk reduction perspective, but the cost of implementation may be prohibitive.
- *Compatible with agencies objectives?* – The options selected need to be compatible with the overall objectives of the agency. Treatments that are incompatible with existing objectives, culture, or policies are obviously unacceptable, no matter how effective they might prove.

**Prepare and Implement Treatment Plans**

The purpose of the treatment action plans is to document how the chosen options will be implemented. These plans should include the following:

- *Proposed actions* – What is the selected treatment?
- *Resource requirements* – What is required to implement the treatment?
- *Responsibilities* – Who has responsibilities to implement the treatment – i.e., Treatment Owner?
- *Timing* – What are the timeframes for treatment implementation?
- *Performance measures* – What are the key indicators that will demonstrate the progress of implementation and ultimately the effectiveness of the treatment option?
- *Reporting and monitoring requirements* – Who needs to be informed during and at completion of the implementation of the treatment? How will the implementation be monitored?

A treatment becomes a control only when it has been 100% implemented and signed-off by the Treatment Owner. It is then subject to controls assurance and the regular monitoring and review process. Following the implementation of the treatment options, the level of risk needs to be re-evaluated to determine if the treatment brings the risk to an acceptable level for the organisation or agency. If not, further treatment options may need to be selected.

# 8. Monitoring and Review

Risk management is dynamic, iterative and responsive to change. Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

As with communication and consultation, monitoring and review is an on-going part of risk management that is integral to every step of the process. It is also the part of risk management that is most often given inadequate focus, and as a result the risk management programs of many organisations or agencies become irrelevant and ineffective over time. Monitoring and review ensures that the important information generated by the risk management process is captured, used, and maintained.

Monitoring and review are related processes, but the distinctions between them are important in the context of risk management:

'**Monitoring**' is an ongoing process of routine surveillance of both internal and external environments.

'**Review**' is a more periodic process that looks at the current status or situation, and usually has a specific focus.

Monitoring and review should be designed to detect both gradual and sudden change. Continuous monitoring is most likely to detect a dramatic change in a timely fashion, whereas periodic review of a particular aspect of the risk process is more oriented towards detecting trends and incremental change.

Part of the strategy and process of monitoring risk is to hold internal and/or external audits from time to time. Audits help an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Organisations must follow their own internal **auditing requirements** as well as any statutory or regulatory obligations to conduct audits. Establishment of an audit and risk committee and the consistent application of a 'model charter' might be some of the internal frameworks that apply to an organisation's auditing set-up.

### Focus Areas

Monitor and Review procedures are focused on two principle areas of risk management. The first area relates to issues specific to a particular risk assessment, which would cover the following:

· *Context* – the risk assessment context, which was established from a number of facts and deductions. For instance, the operational environment, organisation or agency structure, stakeholder expectations, statutory requirements, economic conditions and political environment are all based on perceptions at the time. The monitoring and review process should detect if any of these underlying assumptions have changed, or if new factors have emerged that impact upon the context of the particular risk assessment.

· *Risks and Controls* – numerous factors can cause the likelihood and consequences of risks, or the actual nature of the risks themselves, to change. The controls for risks can also become less effective or irrelevant. Monitoring by the risk owner and others will ensure the timely detection of these changes so that appropriate action can be taken.

· *Treatments* – risk treatments need to be monitored and reviewed to ensure they are fully and correctly implemented. In some cases, treatments need to be adapted or strengthened because the risk they are designed to address has changed; in other instances, resources can be saved by discontinuing irrelevant treatments.

The second area for monitor and review is the application of the risk management process across the entire organisation or agency, with specific attention to the following:

· Consistent application of the Risk Management process across the agency

· Incorporation of the Risk Management process into Strategic, Operational and Project/Event planning

· Adoption of risk management practices and procedures by staff at all levels

### Roles and Responsibilities

The monitoring and review of an organisation's or agency's risks is an integral part of all core business functions, and it should be seen and treated as such. (Refer RG 205.32–39.)

The monitoring and review of the specific risk contexts, actual risk, controls and treatment is primarily the responsibility of Risk and Treatment Owners and be should be integrated into the existing reporting lines and forums of the organisation or agency.

The monitoring and review of the application of the organisation's or agency's risk management policy and procedures should be integrated into the role of Senior Management, who should then ensure that the process is effective in delivering the desired outcomes. Internal and External audit may also play an important part in verifying application of the risk management process.

Risk management should be fully incorporated into the operational and management processes at every level of an organisation or agency.

A final comment with regard to monitoring and review is the important role it plays in good corporate governance. All organisations or agencies face increasing requirements for sound and transparent decision-making and prudent allocation of resources. The monitoring and review process is pivotal in fulfilling these requirements. A structured Risk Management process provides a means for senior executives and directors to stay informed about the risks associated with an organisation's or agency's activities and to ensure appropriate measures are in place to address those risks. It contributes transparency and objectivity to decision-making, and it provides an audit trail to demonstrate how those accountable officers have fulfilled their obligations to provide good governance.

### Sample Risk Register

All Risk Identified and sorted by Level of Risk.

| Risk Ref. Number | Directorate | Division | Department | Activity | Risk | Control Rating | Risk Level |
|---|---|---|---|---|---|---|---|
| 257-1 | Risk Management Commission | Information Technology | Information Technology Section | Maintenance of existing Systems | Inadequate IT system – does not meet the needs of the business | Inadequate | 20 |
| 257-8 | Risk Management Commission | Human Resources | Human Resources Section | Maintain Sustainable and Skilled Workforce | Inability to provide adequate skill mix to deliver services. | Adequate | 20 |

| Risk Ref. Number | Directorate | Division | Department | Activity | Risk | Control Rating | Risk Level |
|---|---|---|---|---|---|---|---|
| 256-2 | Risk Management Commission | Human Resources | Human Resources Section | Recruitment | Failure of recruitment staff to comply with HR policies and procedures. | Inadequate | 16 |
| 256-4 | Risk Management Commission | Human Resources | Human Resources Section | Recruitment | Non-compliance with Public Sector Standards in HR Management & Ethical codes. | Inadequate | 16 |
| 256-10 | Risk Management Commission | Human Resources | Human Resources Section | Maintain Sustainable and Skilled Workforce | Inadequately skilled staff. | Adequate | 16 |
| 257-2 | Risk Management Commission | Information Technology | Information Technology Section | Maintenance of existing Systems | Business interruption due to failure of IT system | Adequate | 16 |
| 257-3 | Risk Management Commission | Information Technology | Information Technology Section | Information Management and Use | Inadequate technical support. | Excellent | 15 |
| 256-11 | Risk Management Commission | Human Resources | Human Resources Section | Maintaining a Safe Working Environment | Failure to comply with legislation and Act. | Adequate | 15 |
| 259-2 | Risk Management Commission | Operations | Operations Section | Reporting | Reports non-compliant due to lack of knowledge of government requirements | Adequate | 15 |
| 259-1 | Risk Management Commission | Operations | Operations Section | Budget Planning | Inadequate funds to fulfil Operational requirements. | Inadequate | 6 |

*Source:* RiskCover, *Risk Management Guidelines*, First Edition, Western Australian Government, Perth.

# 9. Risk Management Checklist

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

This approach will enable a risk management initiative to deliver outputs, including compliance with applicable governance requirements, assurance to stakeholders regarding the management of risk and improved decision-making. The impact or benefits associated with these outputs include more efficient operations, effective tactics and efficacious strategy. These benefits need to be measurable and sustainable. Table 11 provides a checklist of actions that should be completed in order to fully satisfy risk management requirements.

A summary of the risk management requirements that should be in place in order to ensure good standards of risk governance are presented by way of the following checklist:

**Table 11: Risk Management Checklist**

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

*Source:* AIRMIC, Alarm, IRM, *A Structured Approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*, Institute of Risk Management, United Kingdom, 2010.

# 10. Bibliography


Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Commonwealth of Australia, 2006.

Australian Competition and Consumer Commission, 'ACCC proposes to allow self-regulation for mortgage industry association ', ACCC, viewed 10 November, 2010, <http://www.accc.gov.au/content/index.phtml/itemId/407949/fromItemId/378016>.

Australian Securities and Investments Commission, *New Credit Laws and Book up: What you need to know*, ASIC, June 2010.

Australian Securities and Investments Commission, *Regulatory Guide 205: Applying for and varying a Credit Licence*, ASIC, June 2010.

Australian Securities and Investments Commission, *Regulatory Guide 205: Credit licensing: General Conduct Obligations*, ASIC, June 2010.

Australian Securities and Investments Commission, *Regulatory Guide 206, Credit licensing: Competence and Training*, ASIC, June 2010.

Australian Securities and Investments Commission, *RIS-RG206 ASIC Implementation of the National Credit Act: Training and Competence of Credit Licensees*, ASIC, December 2009.

Australian Securities and Investments Commission, *Regulatory Guide 207, Credit licensing: Financial Requirements*, ASIC, June 2010.

Australian Securities and Investments Commission, *Regulatory Guide 209, Credit licensing: Responsible lending conduct*, ASIC, June 2010.

Allens Arthur Robinson, *Focus: National Consumer Credit Protection Reform Package introduced 1 July 2009*, viewed 26 October, 2010, <http://www.aar.com.au/pubs/ baf/fobafjul09.htm>.

Australian Prudential Regulation Authority, *Protecting Australia's Depositors, Insurance Policyholders and Superannuation Fund Members*, Commonwealth of Australia, 2010.

Australian Prudential Regulation Authority, *Annual Report 2010*, Commonwealth of Australia, 2010.

Australian Prudential Regulation Authority, *Annual Report 2011*, Commonwealth of Australia, 2011.

Berrigan Doube Lawyers Group, *Australian Credit Licensing: A New Regime*, viewed 12 November 2010, <http://www.bdlg.com.au/index.php/Commercial-Business-Law/australian-credit-licensing-a-new-regime.html>.

Brookfield, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, viewed 27 October 2010, <http://www.brookfieldmultiplexcapital.com/investment-funds/for-advisers/ anti-money-laundering-and-counter-terrorism-financing-act-2006/>.

Corrs Chambers Westgarth, *Anti-Money Laundering and Counter-Terrorism Financing Bill 2006*, viewed 27 October 2010, <http://www.corrs.com.au/corrs/website/web.nsf/Content/ Pub_InBrief_AntiMoneyLaunderingandCounterTerrorismFinancingBill2006>.

*Fair Trading Act 1999*, Parliament of Victoria, 1999

Finance Brokers Association of Australia Ltd, *Code of Practice & Disputes resolution Service*, viewed 26 October 2010, <http://www.financebrokers.com.au/code_of_practice/ introduction_2>.

Finance Brokers Association of Australia, *Submission on Anti-money Laundering and Counter Terrorism Revised Exposure* Draft ("The Revised Bill"), FBAA, 2006.

Finance Brokers Association of Australia, *Submission on Australian Government Productivity Commission Draft Report of Review of Australia's Consumer Policy Framework*, FBAA, 2008

ICA, *2006 General Insurance Code of Practice*, Insurance Council of Australia, Sydney.

*Insurance Contracts Act 1984*, Commonwealth of Australia.

*Insurance Act 1973*, Commonwealth of Australia.

Lavan Legal, *The National Consumer Credit Protection reform package – licensing*, viewed 26 October, 2010, <http://www.lavanlegal.com.au/go/publications/the- national-consumer-credit-protection-reform-package-licensing>.

Legal Access Services Pty Ltd, *National Privacy Principles*, viewed 27 October 2010, <https://www.freelegalaccess.com/content.aspx?id=auprivprinciples>.

Legal Services Australia, *Australian Credit Licences*, viewed 12 November 2010, <http://www.legallawyers.com.au/banking-and-finance-law/australian-credit-licenses/>.

MFAA, *Mortgage & Finance Association of Australia Code of Practice*, v22.07.2010, Mortgage & Finance Association of Australia, New South Wales.

MFAA, *Mortgage & Finance Association of Australia Alternative Forms of Remuneration*, v01.02.2007, Mortgage & Finance Association of Australia, New South Wales

Mortgage & Finance Association of Australia, *Mission and Objectives*, viewed 26 October 2010, <http://www.mfaa.com.au/default.asp?menuid=480>.

*National Consumer Credit Protection Act 2009 (National Credit Act),* Commonwealth of Australia.

*National Consumer Credit Protection Act 2009 (Transitional and Consequential Provisions)*, Commonwealth of Australia.

*National Consumer Credit Protection Regulations 2010*, Office of Legislative Drafting and Publishing, Attorney-General's Department, Canberra, October 2010.

Paul Agnew, *Anti-Money Laundering and Counter-Terrorism Financing Laws – Impact on Brokers, Mortgage Settlements Australia*, 21 September 2006, viewed 12 November 2010, <http://www.mortgagesettlements.com.au/downloads/>.

*Privacy Amendment Act 2000 (Private Sector),* Commonwealth of Australia.

*Privacy Act 1988 Act, No. 119 of 1988 as amended*, Commonwealth of Australia, 2010.

Professional Lenders Association Network of Australia (PLAN Australia), *Our Company,* viewed 26 October 2010, <http://www.planaustralia.com.au/ourcompany/index.htm>

Reserve Bank of Australia, *Banking Services*, viewed 11 November 2010, <http://www.rba.gov.au/fin-services/banking.html>.

Senior Australians Equity Release Association of Lenders (SEQUAL), *Code of Conduct*, viewed 10 November 2010, <http://www.sequal.com.au/content/view/21/38/>.

Status Compliance & Risk Management Consultants, *The National Consumer Credit Protection Act & Australian Credit Licence registration, application and licensing,* viewed 27 October, <http://www.satus.com.au/acl.html>.