Managing Risk

This information sheet defines risk and risk management, outlines the steps to develop and implement a risk management plan and provides links to useful resources.

Risk is something we face every day. Whether we drive a car or walk to work, there is an element of risk. The issue is not the risk itself but the strategies we or society use to ensure that the worst case scenario is less likely to occur and if it does, that the impact is reduced.

We minimise the risk of driving by expecting everyone to prove they have achieved a minimum level of skill and when they can prove this they are awarded a driver's license. We minimise the risk of walking in cities by providing lights at intersections and expect pedestrians to abide by them when crossing busy streets.

Risk management of an organisation is not dissimilar. Its purpose is to minimise the impact of potential barriers enabling an organisation to achieve its objectives efficiently and effectively.

What is Risk Management?

ISO 31000[1] defines risk management as *"coordinated activities to direct and control an organisation with regard to risk".* Risk management is an integral part of good governance. Ideally it is fully integrated into the governance structure often through delegated responsibility to a committee or an individual who regularly reports to the Board.

Effective organisations systematically identify, measure and manage their risk, understanding whether it is acceptable or requires further action. It assesses whether the level of risk is commensurate with the opportunity it provides. Risk retention for example, where you knowingly accept responsibility for a particular risk, can be acceptable depending on its likelihood and possible consequences in relation to your organisation's purpose and liability. For example, risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. Accepting the risk provides the opportunity to direct the money to support other activities.

Risk management does not create a risk-free environment nor does it encourage an organisation's management to be risk averse. A risk adverse organisation can become inflexible and create barriers to achieving its goals. Equally however, a disproportionate level of high risk could destroy a service.

Ideally, risk management is integrated at all levels of the organisation's processes but particularly in the areas of business and strategic planning, where risk assessment becomes an integral part of decision-making. Some organisations include legal compliance in their risk management plan, others maintain a separate compliance plan.

---

[1] AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines This replaces the Australian Standard AS/NZ 4360:2004 Risk Management

What is Risk?

The ISO 31000[2] standard defines risk as "*the effect of uncertainty on objectives*" where the emphasis is on the effect rather than the event. In risk management the issue is not whether something may unexpectedly happen but that there are plans in place to manage the situation. For example if the CEO or Manager has an accident and is unable to work for a period, the risk will be managed by having strategies in place to ensure the organisation can continue to operate and achieve its objectives with minimal disruption.

Risk arises because organisations operate in environments which include factors we may not be able to control, which in turn can generate uncertainty. These factors may assist in achieving objectives but can also interrupt or prevent them happening. For example, the equal remuneration case may improve wages and therefore make it easier for organisations to recruit and retain qualified staff however it may also impact on service levels.

Compliance and risk management

Failing to comply with legislation is clearly a risk however there is an argument that these risks need to be treated separately under a legal compliance plan, as opposed to a risk management plan. The Australian Centre for Philanthropy and Nonprofit Studies at Queensland University of Technology argue that the two are quite separate[3].

Risk management is designed to reduce and manage risk and takes a cost benefit approach, where accepting the consequences of the risk is reasonable. The benchmark for best practice may be set by a number of sources and can be adapted to suit individual circumstances.

Compliance requires that the risk be eliminated or prevented completely. It does not allow for the breach to occur irrespective of the cost. The benchmark is set by legislation and there is no acceptable level of risk.

Benefits of risk management

It assists with decision making and provides a thorough understanding of risk exposure, enabling the organisation to avoid surprises. It improves the chances of achieving organisational objectives and demonstrates due diligence. It allows for improved safety in the work environment, protecting against insurance claims and possible legal action and may reduce your insurance premiums. The information gathered as part of the process can lead to more effective management of assets, activities and programs, while potentially lowering costs and providing greater certainty with budgets. It can provide greater preparedness for change and enhance and protect the organisation's reputation and image.

Sources of risk

There are many sources of risk, the obvious areas being financial, work health and safety and crisis management. Other areas include human resource management, control of your organisation's stock and property but one of the most important areas and often overlooked are reputational risks. Possibly the

[2] ibid
[3] Risk Management and Legal Prescriptions http://www.communitydoor.org.au/risk-management

most important asset a human services organisation has is its reputation. It helps attract funding, staff and volunteers. Damage to its reputation can destroy an organisation. Such risks need to be identified and managed.

Risk management framework

According to ISO 31000[4] there are five key components of a risk management plan. These are:

- **Mandate and commitment** This is an ongoing activity which is owned by the Board, implemented by senior staff and supported by all.
- **Design of framework for managing risk** It includes a risk management policy which will embed processes into practice, assign resources and clarify responsibility for all aspects of the plan. It will also include a communications and training strategy, with a reporting schedule to ensure effective implementation.
- **Implementing risk management** This is putting the theory into practice. The risk owners (the people with the accountability and authority to manage risk) show they understand and act on their responsibilities ensuring that strategies for managing risk are integrated into all decision making and business processes.
- **Monitoring and review** It ensures that the risk management activities and processes are actually working effectively and any gaps are identified and addressed.
- **Continual improvement** An effective framework is regularly reassessed and enhanced as required. It is a continuous process not an annual event.

Process to develop a risk management framework

The process itself involves five steps[5]. The first three build on each other, whilst *Communication and consultation* and *Monitoring and review,* both need to occur throughout the process.

Establishing context

This includes identifying your organisation's objectives (vision, mission, goals, etc), the environment you operate in and the factors which influence your effectiveness. These factors can include financial, political, operational, cultural, public perception, legal, etc. Tools such as SWOT[6] and PEST[7] analyses can assist this process, as can an inspection of the workplace and a review of work practices. This provides information about the organisation but also its capability and the strategies it relies on to fulfill its objectives. It is used to set the scope, define the objectives of the risk management process and develop risk criteria tailored to the organisation's needs.

---

[4] Ibid

[5] See References and Resources for more detailed information and templates to support the development and implementation stages of this process.

[6] Strengths, Weaknesses, Opportunities, Threats Analysis

[7] Political, Economic, Socio-Cultural, and Technological Environmental Analysis

Risk assessment

Includes three steps:

- **Risk identification** Identifies possible risk, their sources and potential impacts. The sources will assist development of preventive risk treatment and the impacts will assist development of reactive strategies.
- **Risk analysis** Identifies controls, including those already in place and assesses their actual or potential effectiveness.
- **Risk evaluation.** Considers questions such as what is an acceptable or intolerable level of risk, which risks need treatment and what are the priorities?

Risk treatment

Having identified and analysed the risk, it is necessary to identify the most appropriate treatment. This can include controlling the risk (eg two signatures on cheques), reducing the likelihood (eg quality assurance programs), reducing the consequences (eg staff training), transferring the risk (eg insurance), accepting the risk (eg employing staff) and avoiding the risk (eg discontinue the service).

Communication and consultation

Communication and consultation needs to involve both the Board and staff (ie key stakeholders) and where appropriate volunteers, members and/or clients, allowing the process to be both transparent and inclusive.

Consultation will help identify the risk management context, the risks themselves and potential treatments. It is equally important in the monitoring and review processes.

One of the key areas in relation to communication is the development of a shared vocabulary to ensure that everyone is using the same terms in the same way ie when something is described as a low risk, there is agreement on what this means. Reports, memos, written procedures, verbal updates and training are all important aspects of communication.

Monitoring and review

Ideally this will be planned and regular, not simply an annual event but integrated into all major decisions. It will identify new risks and assess the effectiveness of current risk treatments. It will involve consultation with stakeholders and require regular reporting to the Board.

Who is responsible?

Risk management is a governance activity and as such it is ultimately the responsibility of the Board. Often one individual will oversee the process on behalf of the Board. This may be a Board member or senior staff member, however it must be someone who has the delegated authority and accountability to manage risk. The position will need to report regularly to the Board, whilst keeping staff informed of progress.

Alternatively, many organisations establish a Risk Management Team that reports to the Board and designs the process, implements the plan and monitors its progress, ensuring that management of risks is an

integral part of planning, management processes and the organisation's culture. The team would typically comprise of at least one Board member and one senior staff member. It would be expected to report regularly to the Board.

The role of the Board is to make final decisions regarding implementing, monitoring and reviewing the risk management plan.

References and Resources

NCOSS Sector Support

- Templates and Resources
  - Board Delegations
  - Good Governance
  - Managing Conflicts of Interest
  - Probity and Governance
  - Protecting Your Organisation Against Fraud
  - Strategic Planning

Insurance

- Insurance: What's it all about? (2nd Ed) NCOSS 2015

Risk Management Standards and related documents

- SAI Global Publications
  - AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines
  - Guide 73:2009 Risk Management - Vocabulary
  - HB 266:2010 – Guide for managing risk in not-for-profit organisations

- Purdy, Grant (2009) Raising the standard – the new ISO risk management standard .
  This is a comparison of the current standard with the previous Australian Standard *AS/NZ 4360:2004 Risk Management*

NSW Family and Community Services (FACS)

- Risk management Chapter 7 in Good Governance: It's your business
  (Includes checklists, tools for identifying risk levels, sample risk policy, etc)

Community Door

- Risk management –
  (Includes detailed steps to identify risk factors and levels and identify treatments, including tools and templates)

Government of South Australia

- Risk Management for Volunteers
  (Includes templates and tools to identify risk and detailed information on the process)

Human Services Victoria Volunteering Portal

- Health and safety in "I can do that"
  (Includes detailed steps to identify risk factors and levels)

Board Connect

- The Finance, Audit and Risk Management Committee - Terms of Reference
- Risk Analysis
- Steps in a Risk Management Strategy
- Legal Duties of Board Members
- Directors and Officers Liability Insurance
- Risk in Non-Profit Operations
- Legal and Governance Best Practice and Compliance
- Health and Safety Leadership Checklist

Governance Institute of Australia

- Risk Management Policy – Governance Institute of Australia
  (Outlines what a risk management policy should include)

NB: The above websites were accessible on 17 August 2015. If the links do not work search on the title of the document or go directly to the organisation's website.