Ashfield Council

# Risk Management Procedures

March 2013

These procedures will be reviewed triennially by:

Next review date: March 2016

| | |
|---|---|
| **Title:** | Risk Management Procedures |
| **Summary:** | These procedures support the implementation of Council's Risk Management Policy and form part of Council's overall risk management and governance frameworks. |
| **Record Number:** | 2011 |
| **Date of Issue:** | March 2013 |
| **Approval:** | Council |
| **Version Control:** | Adopted by Council on 27 September 2011<br>Revised and adopted by Council, March 2013 |
| **Contact Officer:** | Director, Corporate and Community Services |
| **Relevant References:** | Ashfield Council Risk Management Policy<br>Ashfield Council Risk Register<br>Ashfield Council Hazard Identification and Risk Assessment (HIRA) Tools<br>AS/NZS ISO 31000–2009 Risk Management — Principles and Guidelines |
| **Main Legislative or Regulatory References:** | Local Government Act 1993 and Local Government (General) Regulation 2005<br>Work Health and Safety Act 2010 |
| **Applicable Delegation of Authority:** | N/A |
| **Related Ashfield Council Policy:** | Risk Management Policy – September 2011 |
| **Related Ashfield Council Procedure:** | N/A |

## Introduction

Local Government operates in a demanding natural, social and business environment. Today's public sector organisations are faced with a diverse and complex array of potential risks, of which Ashfield Council is no exception. Improving our risk management capability is an organisation wide imperative.

Ashfield Council has a history of very effective practice in the assessment and management of a variety of risks. These Risk Management Procedures will integrate the good work already achieved into a systematic and comprehensive approach to risk management.

Risk management is not risk avoidance. Risk management is more about informed risk-taking. A systematic risk management approach will not restrict creativity or innovation. Risk management is intended to maximise gains and minimise or avoid loss by systematic decision making. It should encourage careful consideration of the full range of options when a decision has to be made.

In developing and applying a risk management approach, we need to consider how to protect the critical elements of our operations from failure while maximising advantage through:

- the consideration of alternative strategies;
- the development of contingency plans;
- careful monitoring and handling of complaints that may signal major difficulties on the horizon;
- recovery planning, to get back on our feet after mishaps; and
- effective coordination where joint action across Directorates and Departments is required to treat a particular risk to which the organisation is exposed.

These Risk Management Procedures will provide the foundation for the integration of risk management into Council policies, processes and activities in a comprehensive manner. They are based on the international risk management standard, *AS/NZS ISO 31000–2009 Risk Management — Principles and Guidelines*.

These procedures outline the introduction of a risk reporting and review process, which will involve all areas across Council. As a starting point, they provide corporate guidance for teams at all levels to take deliberate steps to improve their awareness, assessment, monitoring and treatment of risk.

Vanessa Chan
**General Manager**

## Background

Risk Management Procedures

These procedures aim to provide a comprehensive overview of Council's risk management approach, systems, and processes to assist all Council staff to effectively manage risk.

As there will be few significant activities or initiatives conducted within Council that are risk free, risk management should be a primary competency of all Council managers and staff.

These Procedures will aim to align plans, processes, people, technology and knowledge with the evaluation and management of the risks faced by the organisation so that Council takes a 'whole of business' or 'enterprise-wide' view of risk rather than managing risk in silos.

These Procedures also aim to ensure a consistent, proactive and holistic approach by defining processes and assigning responsibilities.

Risk Management Policy

Council has a Risk Management Policy approved by the Council. This policy sets the tone for Council's risk management approach and establishes the risk management responsibilities of councillors, management and staff.

These Procedures support the Risk Management Policy by further defining the systems and processes necessary to maintain an effective and efficient risk management framework to comply with the Policy.

Benefits of Managing Risk

The benefits of a risk aware culture, regular risk management thinking and managing Council-wide risks will include:

- better decision-making and planning;
- better identification of opportunities and threats;
- proactive rather than reactive management;
- more effective allocation and use of resources;
- improved stakeholder confidence and trust;
- improved compliance with key regulatory requirements;
- better corporate governance; and
- enhanced communication and reporting of risk.

Risk Management Framework

Council's risk management framework includes all the people, systems, policies, procedures and processes that identify, assess, mitigate and monitor all material internal and external sources of risks.

Risk Management Responsibilities

Risk management is a shared responsibility. The activities necessary for a robust risk management function are shared amongst the Councillors, Executive Management, Managers, staff and key service providers.

In accordance with the Risk Management Policy, Council's risk management activities will be co-ordinated by the Manager, Corporate Services utilising other internal resources as appropriate.

## Procedures and Practice

Risk Management Approach

Council will utilise the International Risk Management Standard AS/NZS ISO 31000–2009 Risk Management — Principles and Guidelines to manage risks. This is a structured and proactive approach that can be applied Council-wide to support management of strategic, operational, financial and/or regulatory risks.

Under this approach, there are five key stages to the risk management process.

1. Communicate and consult - with internal and external stakeholders
2. Establish context - the boundaries
3. Risk Assessment - identify, analyse and evaluate risks
4. Treat Risks – implement and assess controls to address risk
5. Monitoring and review – risk reviews and audit

Refer to figure 1 below for an illustration of the AS/NZS ISO 31000–2009 risk management approach.

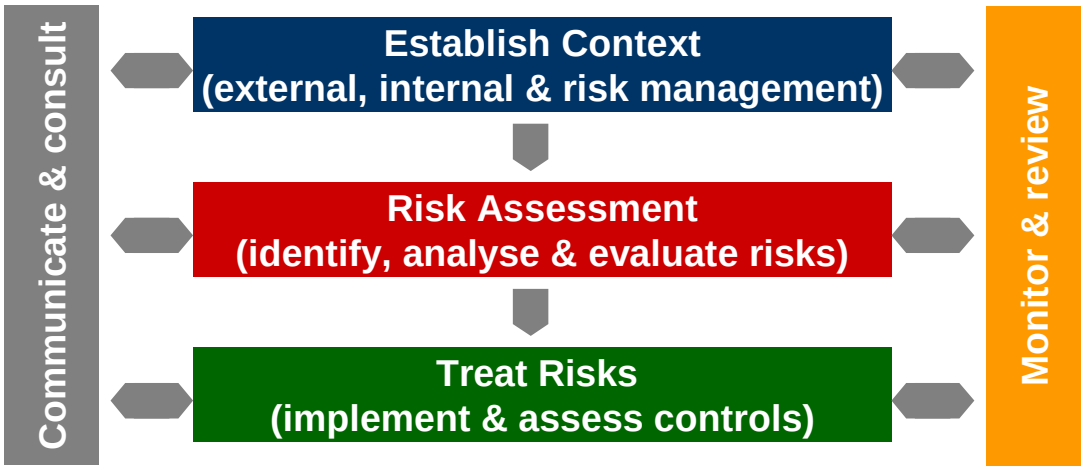


*Figure 1: Our risk management approach using AS/NZS ISO 31000–2009 International Risk Management Standard*

***Establish context***

Establishing the context of risk management at Ashfield Council is the foundation of good risk management and vital to successful implementation of the risk management process.

Context is typically established by the risk leadership team and involves setting boundaries around the depth and breadth of risk management efforts to help Council stay focused and align the risk management framework to relevant matters.

Important considerations when determining context include:

- Council's external environment – social factors, demographics, economic, environmental.
- Council's stakeholders – community, regulators, developers, environmentalists, politicians, unions, media, insurers, service providers, staff and volunteers.
- Council's internal environment – goals, objectives, culture, risk appetite/tolerance, organisational structures, systems, processes, resources, key performance indicators and other drivers.

Considering the nature of Council activities, there will be few significant activities or initiatives conducted within Council that are risk free.

The context of risk management at Ashfield Council will be 'enterprise wide'.

Enterprise risk management is the culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects in order to improve the achievement of enterprise objectives.

This means Council will consider risks across all Council strategies, plans, activities and processes including:

- Management Plans
- Long term strategic plans
- Financial plans and budgets
- Asset management plans
- Social and environmental plans
- Land use plans
- Standard operating procedures

***Risk identification***

Risk identification is the process of identifying key risks facing Council. This involves thinking through the sources of risks, the potential hazards, the possible causes and the potential exposure.

Risk identification occurs within the context of the risk management activity, procedure or process. Council focuses on effective management of the following material risks:

- Strategic risks;
- Operational risks;
- Environmental risks;
- Financial risks;
- Legal and regulatory risks;
- Human resources risks; and
- Information systems risks.

It is important to undertake a systematic and comprehensive identification of key risks including those not directly under the control of Council. The key questions when identifying risks are:

- What can happen?
- Where can it happen?
- When can it happen?
- Why can it happen?
- How can it happen?
- What is the impact?
- Who is responsible?

Council may utilise a number of methods to help identify risks that could materially impact the business, including:

- Brainstorming
- Formal risk workshops and consultation with stakeholders
- Personal experiences
- Expert judgement
- Work review teams/ project teams
- Periodic reviews of the risk register
- Scenario analysis
- Business process reviews
- Review of actual incidents and issues identified
- SWOT analysis

It is also important to consider the potential causes of a risk as it will help to address the risk – which is the next stage of the risk management process. Some causes of risk could include:

- commercial/legal relationships
- socio-economic factors
- political/legal influences
- personnel/human behaviour
- financial/market activities
- management activities and controls
- technology/technical issues
- the activity itself/operational issues
- business interruption
- natural events
- custody of information including the duty to provide and withhold access

### *Risk Analysis*

Once key risks have been identified, they are then analysed. This involves considering and rating the likelihood of occurrence and potential consequences. At this point, no consideration is given to existing controls.

**The likelihood of occurrence** is the probability of an event occurring. When considering the likelihood of a risk, you need to consider both the probability and frequency of occurrence. Council will utilise the following likelihood ratings.

| Likelihood | Expected probability |
|---|---|
| Rare | • No past event history; or<br>• Not expected to occur; or<br>• Would require exceptional circumstances to prevail |
| Unlikely | • No past event history; or<br>• May occur but only in unusual circumstances |
| Possible | • May occur some time but more than likely won't; or<br>• Past warning signs; or<br>• Past history of occurring but very infrequent |
| Likely | • Event will probably occur; or<br>• Past history of event occurring several times |
| Almost Certain | • Occurs often; or<br>• Frequent past history |

*Table 1: Likelihood Ratings*

**The consequence assessment** is the effect or impact of the risk event. It is measured both financially (in terms of profit/loss or balance sheet impact) and operationally (human and physical). Council will utilise the following consequence ratings.

| Consequence | Anticipated impacts |
|---|---|
| Insignificant | • Little or no impact on operations; or<br>• Little or no impact on Council's overall budget; or<br>• Little or no impact on Council's reputation; or<br>• Little or no impact on stakeholders (residents, users, staff etc.) |
| Minor | • Some impact on operations of a very contained and short term nature; or<br>• Minor impact on Council's overall budget (e.g. <$20k; or<br>• Short term and confined impact Council's reputation (e.g. users of a particular service); or<br>• Confined impact on a small number of stakeholders |
| Moderate | • Notable short term impact on operations (e.g. multiple services/activities); or<br>• Substantial impact on Council's overall budget (e.g. in the range of $20-100k, depending on activity); or<br>• Strong interest by local media, short to medium term impact on Council's reputation; or<br>• Impacts a reasonable number of stakeholders |
| Major | • Significant impact on majority of operations, possibly extending for days or weeks; or<br>• Significant impact on Council's overall budget ($100k+); or<br>• Significant legal ramifications; or<br>• Significant impact on Council's ability to meet its compliance requirements; or<br>• Broad negative media coverage, long term reputation impact; or<br>• Impacts a significant number of stakeholders |
| Catastrophic | • Widespread and long term impact on many services; or<br>• Large and unmanageable impact on Council's budget; long term implications; affects Council's financial viability; or<br>• Major legal ramifications; or<br>• Sustained inability to meet Council's compliance requirements; or<br>• Sustained media coverage, irreparable damage to Council's reputation; or<br>• Impacts whole or majority of LGA/stakeholders |

*Table 2: Consequence Ratings*

**Inherent risk** is the overall raw risk. It is determined by combining the likelihood and consequence ratings. Ultimately, the level of inherent risk will determine how a risk is treated. The following table depicts the inherent risk levels that will be used by Council.

| | **Likelihood** | | | | |
|---|---|---|---|---|---|
| **Consequences** | Rare | Unlikely | Possible | Likely | Almost certain |
| Catastrophic | Low | Medium | High | High | High |
| Major | Low | Medium | Medium | High | High |
| Moderate | Low w | Low | Medium | Medium | High |
| Minor | Low | Low | Low | Medium | Medium |
| Insignificant | Low | Low | Low | Low | Low |

*Table 3: Risk Level Ratings*

### *Inherent Risk Evaluation*

Risk evaluation involves comparing the level of risk found during the analysis process against Council's known priorities and requirements.

Depending on the level of inherent risk, treatment strategies will vary:

**Extreme:** Requires immediate action as the potential risk exposure could be devastating to the organisation.

**Very High:** Requires action very soon (within 3 months), as it has the potential to be damaging to the organisation.

**High:** Requires treatment with routine or specific procedures.

**Medium:** Continue to monitor and re-evaluate the risk, ideally treat with routine procedures.

**Low:** Continue to monitor and re-evaluate the risk, ideally treat with routine procedures.

Any risks accorded too high or too low a significance are adjusted, and documented accordingly. The output of the risk evaluation is a prioritised list of risks for further action.

Once each risk has been re-assessed in light of current controls or management strategies, mapping the re-assessed risks onto a matrix will assist in determining whether risks should be prioritised for further action. If the resulting risks fall into the low or acceptable risk categories they may be accepted with minimal further treatment.

Low and accepted risks should be monitored and periodically reviewed to ensure they remain acceptable. If risks do not fall into the low or acceptable risk category, they should be treated using one or more of the options considered below.

### *Addressing Risks*

Addressing risks involves identifying and evaluating existing controls and management systems to determine if further action (risk treatment) is required. Existing controls are identified and then

assessed as to their level of effectiveness. Council will utilise the following control effectiveness ratings.

| Effectiveness | Description |
|---|---|
| Poor | • The control does not address risk<br>• The control is not reliable as it is not well designed, documented and/or communicated. |
| Fair | • Control may be reliable but not very effective as control design can be improved.<br>• Control is reliable but not efficient as documentation and/or communication could be improved. |
| Good | • The control is mostly reliable and efficient. Is documented and understood. |

*Table 4: Control Effectiveness Ratings*

**Residual risk** is the level of risk after considering existing controls. It is determined by applying the effectiveness of existing controls to inherent risk.

Ultimately, the level of residual risk will determine how a risk is treated.

Where controls exist and are considered effective to manage the risk down to medium/low and/or within Council's risk appetite, the residual risk will be low and typically, no further work is required except for periodic monitoring.

Where controls either do not exist or are considered ineffective to manage the risk down to medium/low and/or within Council's risk appetite, the residual risk could be medium to extreme and risk treatment is required. Where Council accepts the remaining residual risk and risk treatment is planned, it is good practice to document the reason why.

| | Control Assessment | | |
|---|---|---|---|
| **Inherent Risk** | Poor | Fair | Good |
| High | High | High | Medium |
| Medium | Medium | Medium | Low |
| Low | Low | Low | Low |

*Table 5: Residual Risk Matrix*

**Risk treatment** involves identifying the range of options for treating unacceptable risks, assessing those options, preparing risk treatment plans and implementing them. Risk treatment options include:

- Eliminating the risk;
- Avoiding the risk (reduce likelihood or consequence);

- Transferring the risk;
- Retaining the risk.

A Risk Treatment Plan should be developed for complex and significant (generally 'High" risk rating or above) risk items shown on the Risk Register.

The treatment plans adopted will be documented and their implementation tracked as part of the reporting process.

***Monitoring and Review***

Few risks remain static. Risks will be continuously monitored and reviewed; and the effectiveness of the controls in place and of the risk treatment plans will be assessed to ensure changing circumstances do not alter risk priorities. Feedback on the implementation and the effectiveness of the Risk Management Policy and Procedures will be obtained from the risk reporting process, internal audits and other available information.

***External Specialists***

Specific and technical risk assessments may sometimes require external expertise. The normal procedures for the engagement of consultants or contractors should apply and Council's insurer also serves as a source of specialist risk advice.

## Roles and Responsibilities

People, specifically managers who are designated 'risk owners' will play a key role in Council's risk management framework. An overview of key risk management responsibilities is set out below.

Councillors

Councillors (or a representative committee of Councillors), with assistance from management and external experts, are responsible for overseeing Council's risk management framework through the normal course of good governance. Responsibilities specific to the risk management framework include:

- adoption of the Risk Management Policy;
- periodic monitoring of risk management systems and processes;
- providing feedback to management on important risk management matters/issues raised by management,
- supporting management in communicating the importance and benefits of good risk management to stakeholders.

Internal Audit Committee

In accordance with its Charter, the Internal Audit Committee is responsible for providing independent assurance and assistance to Council on risk management, including monitoring the control environment to ensure Council's risk management framework is effective.

General Manager

The General Manager is responsible for ensuring risks are managed across all activities and supporting the implementation of the risk management framework by:

- communicating commitment and progress to all staff and relevant stakeholders regularly;
- periodically reviewing risk profiles of Council and ensuring key activities are undertaken in a timely manner;
- reporting known potential risks, emerging risks or major incidents to Council (or a representative committee of Council) in a timely manner;
- ultimately determining if the levels of residual risk are acceptable;
- ensuring that risk management activities are aligned to Council strategy and objectives;
- ensuring sufficient funds are available to support effective and efficient management of risks;
- overseeing processes that help ensure that the operations/activities of Council are compliant with established systems and procedures and regulatory requirements.

Risk Coordinator

The Manager, Corporate Services is Council's designated Risk Coordinator. The Risk Coordinator is responsible for establishing and monitoring the process for the management of risk throughout the Council. The Risk Coordinator is also responsible for:

- ensuring the risk management framework remains relevant and appropriate for Council
- making recommendations on all aspects of the risk management framework to the General Manager, Executive Management, Managers and risk owners;
- providing advice and support on risk management matters;
- providing or coordinating the delivery of appropriate and relevant training to staff to promote a positive risk, compliance and control culture;
- periodically reviewing key risk management related documents including risk register, risk profiles, policies, plans, procedures and authorities;
- periodically reporting the status of key risks and risk treatment plans to the Council executive.

Managers

Managers (and often supervisors) are the risk owners and are required to create an environment where the management of risk is accepted as the personal responsibility of all staff, volunteers and contractors.

Managers are accountable for the implementation and maintenance of sound risk management processes within their area of responsibility in conformity with Council's risk management framework including:

- identifying, recording and periodically evaluating risks;
- identifying, recording and assessing effectiveness of existing controls;
- implementing and maintaining effective internal controls;
- developing treatment plans to treat higher level risks in a timely manner;

- maintaining up to date risk profiles/risk registers through periodic reviews and updates;

Managers are also responsible for supporting good management practices that compliment risk management including:

- complying with and monitoring staff compliance with Council's policies, procedures, guidelines and designated authorities;
- maintaining up to date information and documentation for key operational processes;
- incorporating risk treatment plans into Council's Management, Operational and staff performance plans and budget

Staff

All staff are required to act at all times in a manner which does not place at risk the health and safety of themselves or any other person in the workplace.

Staff support risk owners and are responsible and accountable for taking practical steps to minimise Council's exposure to risks including contractual, legal and professional liability in so far as is reasonably practicable within their area of activity and responsibility.

All staff must be aware of operational and business risks. Particularly, staff should:

- provide input into various risk management activities;
- assist in identifying key risks and controls;
- report all emerging risks, issues and incidents to their Supervisor, Manager or other appropriate Council officer;
- follow Council policies and procedures.

Some positions because of the nature of their roles have additional responsibilities for managing risk, these include the Chief Financial Officer, Insurance and Risk Coordinator and the Director Works and Infrastructure Services.

## Documentation/Recordkeeping

Important risk management processes and activities will be documented throughout Council. Documentation is important for the following reasons:

- it gives integrity to the process and is an important part of good corporate governance;
- it provides an audit trail and evidence of a structured approach to risk identification and analysis;
- it provides a record of decisions made which can be used and reviewed in the future;
- it provides a record of risk profiles for Council to continuously monitor.

Key documents

Key documents will include:

- Risk Management Policy – establishes commitment and provides a high level overview of risk management framework;

- Risk Management Procedures – details the risk management framework processes and activities;
- Risk Register & Risk Profiles – documents the key risks and controls for Council activities and processes;
- Risk Treatment/Action Plans – document strategies to treat risk levels higher than acceptable risk appetite

Maintenance of key documents

Risk documentation including risk profiles, risk registers, written/formal risk assessments, risk/control audits, self-assessments will be maintained in Council's official recordkeeping system.

These records may be called upon in the management of ongoing treatments, as evidence in incident investigations, in dealing with insurance matters or during other inquiries and for audit purposes.

Risk management records should be reviewed:

- on handover of responsibilities between managers
- on assumption of responsibility for a project or program
- bi-annually to match reporting requirements, and
- whenever operating parameters are subject to major change.

## Reporting and Review

Risk Management Framework

Documentation including policies, procedures, risk registers and systems relating to the risk management framework will be subject to periodic review. This review is the responsibility of the Risk Coordinator and should be conducted at least annually.

Risk Register

It is important that risk owners review their risks regularly. Such reviews must be part of the annual management planning process to ensure that:

- risks are managed in the context of each Section objectives for the coming year;
- risk treatment plans are incorporated into the Management/Operational Plans; and
- where funding is required to implement risk treatment plans that it is incorporated into the Council budget process.

Risk Treatment Plans/Action Plans

Risk Owners are responsible for ensuring that actions contained in Risk Treatment Plans (RTPs) are implemented effectively and within agreed timeframes and that they are appropriately documented. In addition, Risk Owners are responsible for ensuring that actions contained in RTPs are included in their Operational Plans and where appropriate Council's Management Plan and staff performance plans.

Risk Status Reports

The Risk Coordinator is responsible for ensuring that Executive Management, Council and the Internal Audit Committee are kept up to date with the status of key risks and RTPs. This will be achieved via bi-annual reports.

Summary of Actions, Reviews and Reports

The following table summarises the key actions, reviews and reports required by Council's Risk Management Framework. It details who is responsible for each activity and the required timing.

| Action | Description | Responsibility | Timing |
|---|---|---|---|
| Review RM Policy and Procedures | Review the currency and effectiveness of Council's Risk Management Policy and Procedures | Risk Coordinator | Every 3 years |
| Review Risk Register | Review risks and controls contained in Council's risk register and identify new or emerging risks | Risk Owners (coordinated by Risk Coordinator) | Every year in November in preparation for the next Management Plan/Budget process |
| Develop Risk Treatment Plans | Develop risk treatment plans for new and emerging risks. | Risk Owners (coordinated by Risk Coordinator) | Every year in November in preparation for the next Management Plan/Budget process |
| Include Risk Treatment Plans into operational planning | Ensure that actions required by Risk Treatment Plans (RTPs) are incorporated into the Management Plan, Operational Plan and staff performance plans | Risk Owners | Every year in accordance with organisational planning process timeframes |
| Implement Risk Treatment Plans | Implement actions contained in RTPs | Risk Owners | As identified in the RTP |
| Conduct specific risk assessments | Conduct risk assessments as required for new or altered activities, processes or events | Risk Owners | As required |
| Risk Status Report | Report current status of key risks and RTPs to Exec Management, Council, Internal Audit Committee | Risk Coordinator | Annually |

*Table 6: Summary of Key Activities*

# APPENDIX 1
# Glossary of Key Risk Management Terms

*Adapted from AS/NZS ISO 31000–2009*

| | |
|---|---|
| **Action Plan** | a plan which sets priorities for risk treatment action responsibilities, timeframes, goal defined, proposed treatment measurers and follow up action. |
| **Abatement** | the process of reducing in amount or intensity any unwarranted consequence. |
| **Consequence** | outcome of an event expressed qualitatively or quantitatively (also both negative – a loss, injury, setback, disadvantage, and positive – a gain, success, windfall). |
| **Enterprise risk management** | the culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects in order to improve the achievement of enterprise objectives. |
| **Event** | incident or situation that occurs in a particular place during a particular interval of time. |
| **Exposure** | an apparently risk bearing condition, issue or incident that has not been subject to risk appraisal and treatment. |
| **Frequency** | measure of the rate of occurrence of an event or outcome expressed as the number of occurrences of the event or outcome in a given time. |
| **Hazard** | a specific source of potential harm or a condition with a known potential to cause loss. |
| **Intelligence** | information which has been subject to judgement, particularly concerning the consequence or impact of an event or outcome and its likelihood. |
| **Likelihood** | a qualitative description of probability or frequency. |
| **Loss** | any negative consequence, financial or otherwise. |
| **Monitor** | to check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change. |
| **Mitigation** | the process and action taken to reduce or moderate an unwanted consequence, to lessen in intensity, force or frequency. |
| **Probability** | likelihood of a specific event or outcome occurring within a designate timeframe. |
| **Recovery** | the measures and process undertaken to return to normal following loss or disaster. |
| **Remediation** | the remedying of a deficiency, especially applied to controlling or minimising hazards. |
| **Residual Risk** | remaining level of risk after risk treatment action has been taken. |
| **Risk** | effect of uncertainty on objectives. Often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence. |
| **Risk Acceptance** | informed decision to accept the consequences and likelihood of a particular risk. |

| | |
|---|---|
| **Risk Analysis** | systematic use of available information to determine how often specified events may occur and the magnitude of their consequence. |
| **Risk Appraisal** | a simplified risk assessment. |
| **Risk Assessment** | overall process of risk identification, analysis and evaluation leading to treatment. |
| **Risk Aversion** | an entrenched dislike of risk bearing situations or circumstances. |
| **Risk Avoidance** | informed decision not to become involved in a risk situation. |
| **Risk Control** | that part of risk management that involves the implementation of policies, standards, procedures and physical changes to eliminate or minimise adverse risks or consequences. |
| **Risk Element** | one operative factor or condition in an exposure or risk bearing activity – *e.g. vehicle condition is one risk element.* |
| **Risk Evaluation** | process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria. |
| **Risk Identification** | process of determining what can happen. |
| **Risk Management** | Co-ordinated activities to direct and control an organisation, including culture, processes and structures. |
| **Risk Management Process** | systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk. |
| **Risk Owner** | Person or entity with the accountability and authority to manage a risk. |
| **Risk Reduction** | selective application of appropriate techniques and management principles to reduce either likelihood of an occurrence or its consequences, or both. |
| **Risk Retention** | intentionally or unintentionally retaining the responsibility for loss or financial burden of loss within the organisation. |
| **Risk Transfer** | shifting responsibilities or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere. |
| **Risk Treatment** | selection and implementation of appropriate options for dealing with risk to contain or reduce consequences to acceptable levels. |