RISK MANAGEMENT POLICY AND STRATEGY

Document Status: Revised

Originator: A Struthers

Updated: E Dyer

Owner: Assistant Director Finance

Version: 01.01.07

Date: 11/01/2024

Approved by Audit & Governance Committee

Document Location

This document is held by Tamworth Borough Council, and the document owner is Jo Goodfellow, Assistant Director Finance.

Printed documents may be obsolete. An electronic copy will be available on Tamworth Borough Councils Intranet. Please check for current version before using.

Revision History

Revision Date	Version Control	Summary of changes
April 2010	1.01.01	
18/09/12	1.01.02	Scheduled review
30/03/14	1.01.03	Scheduled review
03/09/15	1.01.04	Scheduled review
03/08/16	1.01.05	Scheduled review
24/08/17	1.01.06	Scheduled review
11/01/24	1.01.07	Scheduled review/ revision

Approvals

Name	Title	Approved
Audit & Governance Committee	Committee Approval	Yes
CMT	Group Approval	Yes
Joanne Goodfellow	Assistant Director Finance	Yes
Emma Dyer	Operations Accountant	Yes

Document Review Plans

This document is subject to a scheduled annual review. Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be available on the Intranet and the website.

Table of Contents

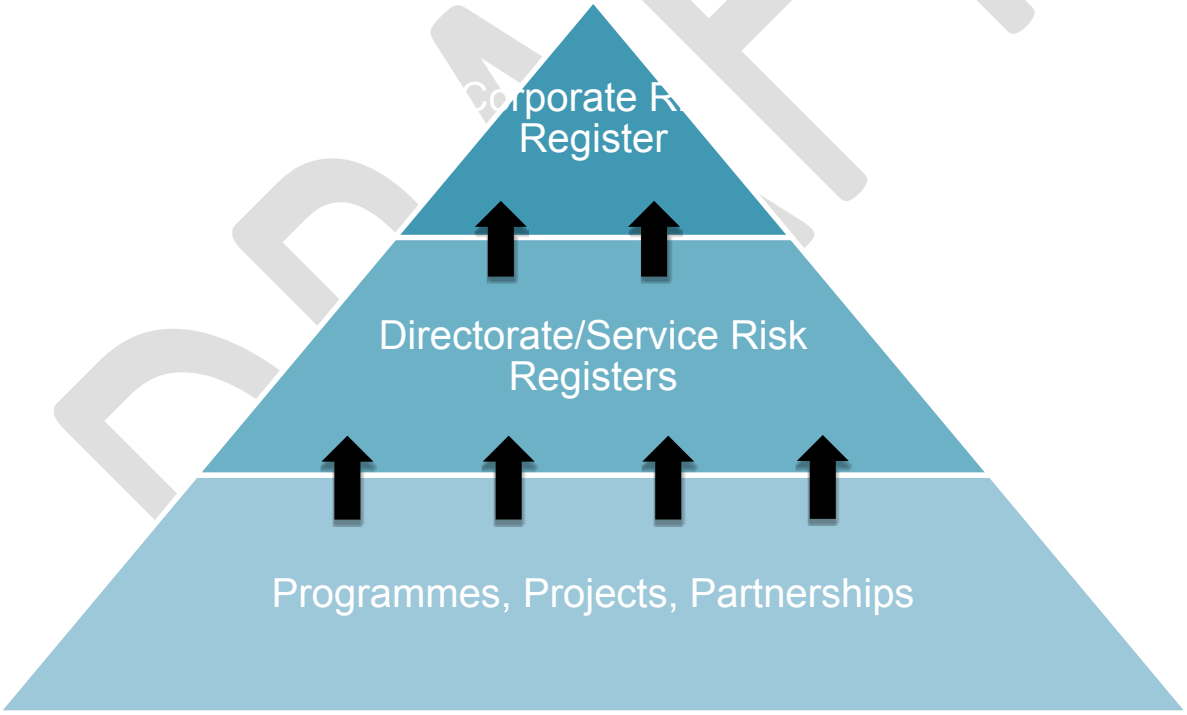
Introduction

All organisations face internal and external factors that can impact on the achievement of their objectives. To be successful our organisation has to understand and respond appropriately to these uncertainties – or risks which could be a threat or opportunity. This strategy and policy document outlines the arrangements and process for understanding these risks and how to decide on appropriate actions to address them.

The risk management process will be used at different levels and in different contexts. These are set out in figure 1, below. The risk registers should relate to the business planning process. For example, the corporate risk register will consider strategic risks to delivery of the Council's Corporate Plan 2022/25, directorate risks will consider operational risks to directorate objectives and so on.

Subsidiary risk registers may also be created and maintained at individual project or partnership level, or as part of the business continuity planning process. Risks should be able to flow between levels to be managed at the most appropriate level.

Figure 1 – Risk Management Structure



Risk Management Policy Statement

Statement by the Leader of the Council and Chief Executive

The Authority is committed to embedding the culture of Risk Management ensuring that its reputation is not tarnished by an unforeseen event nor is it financially or operationally affected by the occurrence.

It recognises that: -

- Management has the responsibility to plan and systematically approach, the identification, evaluation, and control of risk;
- In order for the Authority to improve, risks (opportunities and threats) need to be taken, but they need to be understood and appropriately managed ;
- All Staff Leaders have responsibility for the effective control of risk utilising the support, training and resources provided by the Authority;
- All Staff have the responsibility to manage insurable losses. Insurance is not a substitute for the management of risk.
- There is a need to fully integrate Risk Management into the culture of the Authority.

Risk Management objectives for Tamworth Borough Council are reviewed on a continual basis and reported to CMT and Audit and Governance committee on a quarterly basis. These objectives are designed to:

- To safeguard the public, members and employees,
- To protect the Authority's Reputation, Physical Assets and Services it provides by minimising losses and associated insurance costs;
- To manage risks in accordance with best practice and ensure risk management is integrated into the culture of the Authority and all those connected with it;
- To identify and take advantage of available opportunities to improve service delivery and/or the Authority's financial position;
- To ensure the Authority delivers its commitments to stakeholders and to demonstrate transparency, accountability and equity in its efforts to do so;
- To anticipate and respond positively to changing social, environmental and legislative requirements; and
- To identify and manage partnership risks.

The Audit & Governance Committee will regularly review the Risk Management Policy and Strategy to ensure their continued relevance to the Borough. They will also assess performance against the aims and objectives.

We attach great significance to Risk Management, and it is essential that the Protocol is known and understood by all staff within the Authority. It will form part of the induction training and performance reviews for all staff and members and will be monitored as part of the performance review process utilising the corporate performance system Pentana. We will make adequate resources available to ensure that the commitments made in this statement are achieved.

Risk Management has our total support – it needs yours too for us to succeed.

(Signed)	(Signed)
Chief Executive	Leader of the Council

Policy Objectives

In implementing this Policy the Authority will: -

- Adopt a strategic approach to risk management to make better informed decisions which is vital to successful transformational change
- Identify those assets and exposures which have or may give rise to loss producing events;
- Identify opportunity risks that may give rise to increased benefits
- Maintain detailed 'Risk Registers' of the risks identified as threatening the Authority's operation and document their control on the Authority's Corporate Performance system Pentana;
- Ensure Pentana is routinely reviewed and updated to reflect the Authority's current Risk position
- Quantify the impact of potential loss producing events;
- Take reasonable physical and financial steps to avoid and/or reduce the impact of potential losses and their impact on the Authority's Business Plan;
- Work to reduce all serious (RED) risks to an acceptable level either by controls or ceasing the activity;
- Ensure that all systems of work reflect the positive risk management culture of the Authority;
- Establish a comprehensive information base of insurable and uninsurable losses;

Maintain a detailed understanding of insurance and purchase insurance for those financial risks which cannot be avoided or reduced further, always retaining risks where this is economically beneficial.

Risk Management Strategy

The Purpose of this Risk Management Strategy is to effectively manage potential opportunities and threats to support the Authority in achieving its objectives. The main objectives of the Authority's Risk Management Strategy are to: -

- Achieve continuous improvement in the management of risk;
- Develop a culture that integrates risk management into the day-to-day management process;
- Continue to develop robust systems to identity and evaluate risk;
- Develop reliable performance indicators for target-setting and for making appropriate comparisons;
- Develop systems for performance monitoring to bring about continuous improvements;
- Enabling the Authority to anticipate and respond to changing social, environmental and legislative conditions;
- Reduce the total cost of risk and mitigate potential future increases in insurance premiums and self-insurance options.

To help achieve these objectives it will be necessary to: -

- Increase the profile of and commitment to embedding Risk Management throughout the Authority;
- Ensure adequate resources (financial and time) are provided;
- To make all partners, providers and delivery agents aware of the Authority's expectations on risk, both generally as set out in its Risk Management Policy, and where necessary in particular areas of service delivery;
- Develop arrangements to measure performance of Risk Management activities against the aims and objectives;
- Establish clear accountabilities, roles and reporting lines across all services, departments, management and committees;
- Provide for risk assessment in all decision-making processes of the Authority;
- Develop training to build awareness across all levels of activity;
- Monitor the performance of risk management across the Authority.

- Ensure the Pentana Risk system is the single repository for all managed risks identified across the Authority

Risk Financing Strategy

The Purpose of the Risk Financing Strategy is to effectively manage the financial implications of risk control measures and their impact to maximise the resources available for the provision of Services and the Authority achieving its objectives. The main objectives of the Authority's Risk Management Strategy are to: -

- Reduce the total cost of risk and mitigate potential future increases in insurance Premiums and self-insurance options**.**
- To minimise costs by reducing risks
- To utilize risk self-funding where financially advantageous

Risk Appetite

The risk appetite is *"the amount of risk that an Authority is prepared to accept, tolerate, or be exposed to at any point in time*" (CIPFA).

The Authority will manage the risks by one or more of the following ways:

- Avoid - A decision is made not to take a risk
- Accept – A decision is taken to accept the risk
- Transfer – All or part of the risk is transferred through insurance or to a third party often via a contractual arrangement. This is dependent on the correct use and application of the corporate procurement process
- Reduce – specific actions taken to reduce the risk
- Exploit – A decision is made to exploit opportunities as they arise or are generated.

For both Strategic and Operational risk the Authority has a Low appetite for risk. Despite the low appetite tolerance levels may be higher as it must be recognised that it is not possible to eliminate some of the inherent risks associated with the service delivery activities.

Risk Registers must be maintained and managed in the following areas:

Strategic Risks,

Operational Risks,

Project Risks,

Partnership Risks,

Opportunity Risks

"Severe" risks can appear in any of the above risk registers.

Risks scorings over 12 (Red Risks) will need to be escalated and highlighted to CMT by the responsible officer.

Roles & Responsibilities

The importance of establishing roles and responsibilities within the risk management framework is pivotal to successful delivery. Considering risks must be embedded into corporate policy approval and operational service delivery.

The agreed roles and responsibilities within the risk management framework are outlined in the table below:

Group /Individual	Responsibilities
Corporate Management Team	▪ Provide leadership for the process to manage risks effectively. ▪ Review and revise the Risk Management Policy and Strategy in accordance with the review period. ▪ Monitor and review the Corporate Risk Register on a quarterly basis including the identification of trends, upcoming events and potential new corporate risks.
Audit & Governance Committee	▪ Monitor the effectiveness of the Authority's risk management arrangements, including the actions taken to manage risks and to receive regular reports on risk management. ▪ To monitor the actions being taken to mitigate the impact of potentially serious risks
Cabinet	▪ To provide strategic direction with regard to risk management. ▪ To ensure risks are taken into consideration for Committee and Council decisions.
Assistant Directors	▪ To provide leadership for the process of managing risks within their directorate.

	▪ To ensure that risk management methodology is applied to all service plans, projects, partnerships and proposals within their directorate. ▪ To identify and manage business /operational risks. ▪ To ensure that the management of risk is monitored as part of the performance management process.
Heads of Service	▪ To ensure that all risks are identified, recorded and effectively managed in their area or responsibility. ▪ To review and update their risk register on at least an annual basis but appropriate to the risk. ▪ To determine the method of controlling the risk. ▪ To delegate responsibility if appropriate for the control of the risk. ▪ To notify the Assistant Director of new risks identified for consideration for inclusion on the corporate risk register.
All staff	▪ To ensure that risk is effectively managed in their areas. ▪ To ensure that they notify their managers of new and emerging risks.
Assistant Director Finance / Operations Accountant	▪ To ensure that the Risk Management Strategy is regularly reviewed and updated. ▪ Promote and support the risk management process throughout the Authority. ▪ Advise and assist managers in the identification of risks. ▪ The Assistant Director Finance will ensure that all Managers are aware of their responsibility for Risk Management. ▪ The Assistant Director Finance will be responsible for ensuring that the Risk Strategy of the Authority is achieved. ▪ The Operations Accountant will be responsible for the administration of risk and insurance and the co-ordination of advice and support of the Authority is achieved.

Risk Management Definitions

a. Definitions

'Risk' is defined as the "effect of uncertainty on objectives" (ISO 31000). An effect is a positive or negative deviation from what is expected, and that risk is often described by an event, a change in circumstances or a consequence.

'Risk Management' refers to a coordinated set of activities and methods that is used to direct an organisation and to control the range of risks that affect its ability to achieve objectives.

A 'Risk Management process' is one that systemically applies management policies, procedures, and practices to a set of activities intended to establish the context, communicate and consult with stakeholders, and identify, analyse, evaluate, treat, monitor and review risk.

b. Benefits of Risk Management

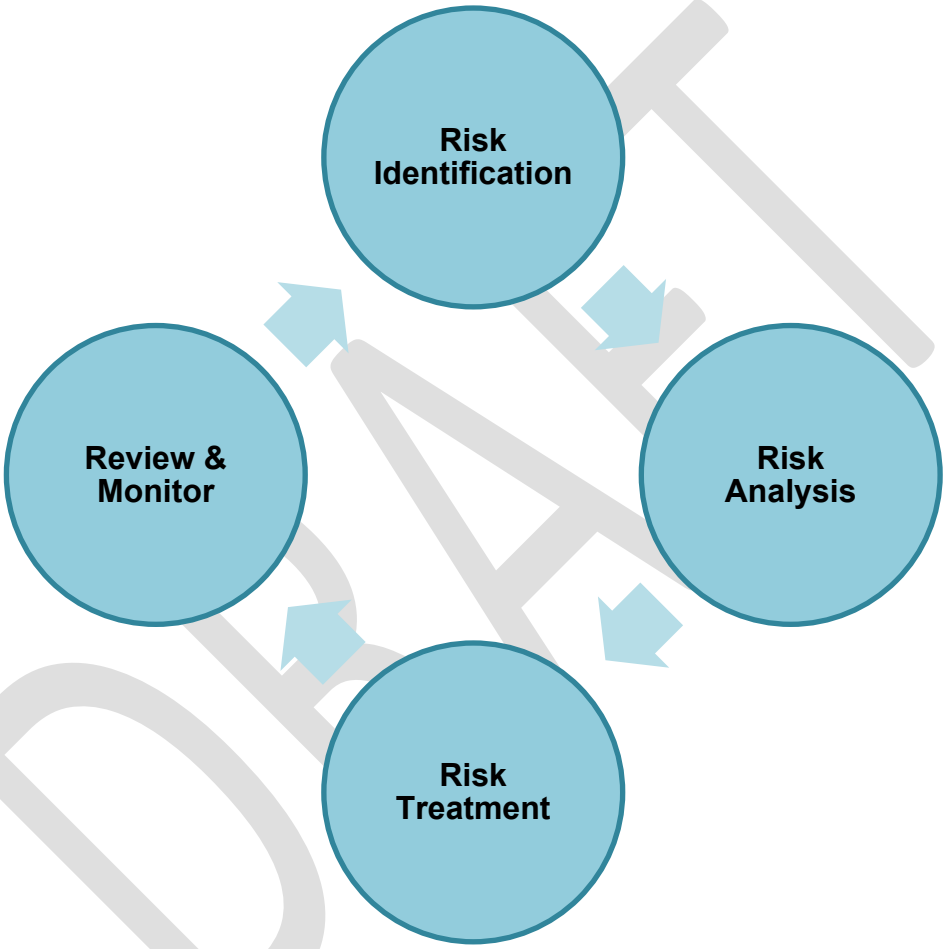
Risk Management is an integral component of corporate governance in maintaining a strong control environment.

- Risk Management activities are designed to ensure that an organisation complies with legal and regulatory obligations, as well as customer requirements.
- Risk Management activities provide internal and external stakeholders with assurance that significant risks have been identified and appropriate controls put in place.
- Risk Management activities provide additional structured information to assist with decision making.
- Risk Management activities enhance the effectiveness and efficiency of operations within the organisation and ensure business processes (by way of tactics, projects and other change initiatives) are also effective and efficient.

Risk Management Process

The risk management process has 4 steps as outlined in figure 2, below. Underpinning each stage of the process is communication and consultation with interested parties and stakeholders. This supports ensuring internal and external stakeholders are considered and involved in the Authority's work to understand and define its risks.

Figure 2 – Risk Management Process



a. Risk Identification

The identification of risks is completed at various levels and primarily, risks (and opportunities) relate to the achievement of the Authority's objectives. The objectives can be Strategic, Operational, Project or Opportunity level. This stage can be repeated regularly to ensure that new risks arising are identified and recorded on the risk register as appropriate.

The Authority acknowledges that no one person is responsible for identifying key risks and that they are identified at various levels and in various ways.

As a basis, the following risks must be identified:

Those that affect:

1 the delivery of the Strategic Plan;

2 the operational issues i.e. the delivery of a service;

3 the delivery of a project;

4 the delivery of a Partnership arrangement

Risks can be identified in a number of forums, including:

- A workshop session with management teams having open discussions
- Interviews with responsible individuals
- Meetings with smaller groups of officers (Risk Champions Meetings)
- Questionnaires

Sources of information that could help inform risk identification include:

- The Council's Corporate Plan and Directorate or Service plans
- Strengths, weaknesses, opportunities and threats (SWOT) analysis
- PESTLE analysis (Political, Economic, Social, Technological, Legal, Environmental)
- Performance reports
- Internal or external research papers or statistical trends
- Risks or issues raised by audit or any other internal/ external scrutiny body
- Risks identified through budget setting process
- Health & safety/ business continuity risk assessments
- Partnership, programme or project documentation (e.g. business case or project risk register)

It is crucial for risks to be defined and articulated properly at this stage including understanding the key causes and potential consequences of the risk. Failure to do so can result in confusion about the exact nature of the risk, ineffective risk controls being implemented, or the risk analysis being over or underestimated. A concise structured risk description would take the following format:

Failure to X (cause), Y may happen (risk event), resulting in Z (consequences).

Example: *"Failure to plan and be prepared (X) for extreme weather impacts (Y) may result in flooding and other damages (Z)."*

b. Risk Analysis

Once identified the risk matrix (see Figure 3, below) is the main tool for assessing each risk on the Pentana system. The analysis also helps prioritise each risk so we know which risks are most significant and therefore are in need of greater attention, effort and resources. It also allows us to compare different types of risk with each other.

Each risk should be analysed for the likelihood it will happen and the impacts if it did happen. This assessment should be made considering controls that are already in place and working effectively. Probability assessment is applied relative to specific timeframes e.g. 'operational' risks will be assessed over a shorter timeframe than 'strategic' risks.

Likelihood Criteria:

- 4 – Very likely
- 3 - Likely
- 2 - Unlikely
- 1 – Very unlikely

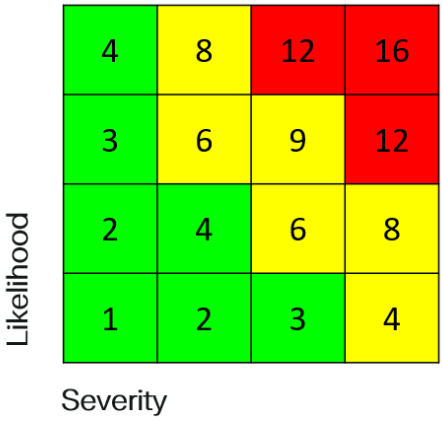
The impact should be considered against the relevant objectives - corporate risks should be scored against the council's objectives; directorate risks scored against directorate objectives; service risks scored against service objectives; project risks scored against the objectives of the project. The impact relates to the potential effects on an objective, activity or function which may either be positive or negative.

Impact Measure: There are 4 'impact descriptors' as follows:

- 4 - Major
- 3 - Serious
- 2 - Significant
- 1 - Minor

Each identified risk should be assessed at the Original (Inherent), Current (residual) and Target level.

Figure 3 – Risk Matrix



c. Risk Treatment

The Risk Treatment step is about putting in place appropriate controls or mitigation for each risk. It is about turning the knowledge gained about each risk into appropriate action – to treat or not to treat the risk. The risk identification will inform any specific actions needed.

There are four treatment options available if the judgement of the risk is **further treatment of the risk is needed:**

- **Treat**: to take one or more actions that could reduce the potential likelihood or impact or both of a risk occurring or to mitigate the effects of the risk should it manifest.
- **Tolerate**: where the effects are likely to be within the identified risk tolerances, the risk owner can 'tolerate' the risk assuming they have the authority to do so.
- **Transfer**: to move or transfer the effects of a risk to a third party e.g. purchasing insurance, outsourcing, contractual transfers etc.
- **Terminate**: to 'terminate' the action that gives risk to the risk e.g. to stop an activity, close down operation, programme etc.

Specific actions agreed to further treat risks should be recorded on the relevant risk register with an appropriate timeframe agreed for implementing them. A model to use that supports action(s) implementation is the SMART model – Specific, Measurable, Achievable, Realistic, Timely.

All risks should be allocated a 'risk owner'. The risk owner will be responsible for monitoring the risk and co-ordinating any actions needed to manage the risk.

d. Review & Monitor

Each directorate or service area is responsible for updating and maintaining its own risk register. Monitoring and review of these risk registers should be done at least quarterly. However individual directorates, services, or officers may choose to monitor and review their risk registers more frequently or on an ad hoc basis between quarterly reviews.

Partnerships and projects should agree their own monitoring cycle. This should be determined by the level of risk and the pace of change to the risks. It is expected however that significant partnerships and projects will review risk registers at least quarterly.

Service risk registers should be challenged through the directorate management team and/ or other appropriate review process.

When any team reviews risk registers the following should be considered:

- Have existing risks changed in any way?
- Has the likelihood or impact score changed since the last review?
- Have further actions, if they were needed, been implemented?
- Are the controls in place to manage the risk effective and still working adequately? What assurance is available to support this judgement?
- Are the controls in place appropriate to the level of risk?
- Is the response overly cautious or is more attention needed?
- Have all interested parties or stakeholders been consulted on the risk or communicated with in an appropriate way?
- Are there any new or emerging risks not captured in the risk register?

Are there any risks that can be deleted or removed from the register?

Recording Risks

A Risk Register is the primary tool to administer the risks identified. The Pentana system **must** be used to record all Strategic and Operational, project and partnership risk registers.

As part of business planning, risks are identified and Managers should ensure that the associated risks are recorded on the risk register held within the Pentana system and linked to the appropriate business plan action.

All risks recorded on the risk register should identify the:

- Gross risk,
- Vulnerabilities/causes of the risk,
- Potential effect/consequences of the risk happening,
- Controls in place to reduce the risk, or action plan with to introduce control these items to carry specific completion dates
- Residual risk,
- Risk review period.
- Target risk, to reflect the acceptable level of risk for the issue identified.

Reporting Risks

The Corporate Risk Register will be reviewed and updated by the Corporate Management Team on a quarterly basis and then reported to the Audit & Governance Committee.

All reports to any Committee of the Authority require that risks are identified. The Committee report template is set up so that this is completed. It is the duty of the report writer to ensure that the relevant risk register on Pentana is updated to take account of these risks.

Escalating/ de-escalating the risk

A decision may also be taken at this time to escalate or de-escalate the risk, for example from a project manager to a sponsor or from a directorate to the executive. The following criteria may help this decision:

- The level of confidence the risk is fully understood
- Risks outside of the directorate, partnership or project's risk appetite
- Risks of a corporate or cross cutting nature, for example an IT or HR risk that could have significant consequences for others in the Council
- The risks requires co-ordinated action across the Council to manage it effectively

Performance Management

The following key performance indicators for the risk management process will be completed.

- The Risk Management Policy and Strategy to be reviewed and updated on an annual basis;
- Corporate Management Team to review and update the Corporate Risk Register taking into account emerging and changing risks on a quarterly basis;
- Risks to be reviewed appropriately to the severity /changing nature of the risk;
- Staff to be appropriately trained in Risk Management and the use of the Pentana system.

Appendix 1 Terminology

The terminology used is based on ISO31000, 'Risk Management Standard'. The list is iterative and will be developed further over time:

Term	Definition
Consequence	Is the outcome of an event and that has an effect on objectives. A single event can generate a range of consequences which can have both positive and negative effects on objectives. Initial consequences can also escalate through 'knock-on' effects.
Control	A control is any measure or action that modifies risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or manages risk. Risk treatments become controls, or modify existing controls once they have been implemented.
Event	An event could be one occurrence, several occurrences, or even a non-occurrence (when something doesn't happen that was supposed to happen). It can also be a change in circumstances. Events can also be referred to as incidents or accidents and always have causes and usually have consequences.
Original (Inherent) Risk	The probability and impact of a loss arising out of a potential event or which exists in an environment, in the absence of any action to control or modify the effects.
Likelihood	'Likelihood' is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively.
Monitoring	To monitor means to supervise and to continually check and critically observe. It means to determine the current status and to assess whether or not required or expected performance levels are being achieved.
Operational Risk	Risk of loss or gain, resulting from inadequate or failed internal processes, people, and systems or from external events' and capable of impacting the operations of the organisation.
Current (Residual) Risk	The residual risk is the risk left over after you've implemented a risk treatment option, also known as 'residual', risk. The 'current' risk is the risk remaining after you've reduced the risk, removed the source of the risk, modified the consequences, changed the probabilities, transferred the risk, or retained the risk.
Review	A review is an activity carried out in order to determine whether something is a suitable, adequate, and effective way of achieving established objectives.
Risk	Is the effect of uncertainty on achieving an objective or objectives.
Risk Analysis	Process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. Risk analysis is also used to study impacts and consequences and to examine the controls that currently exist. How detailed your risk analysis ought to be will depend upon the risk, the purpose of the analysis, the information available and the resources available.
Risk assessment	Risk assessment is a process comprising three stages, i.e., risk identification, risk analysis, and risk evaluation. – Risk identification is used to find, recognize, and describe the risks that could affect the achievement of objectives. – Risk analysis is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that currently exist. – Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.
Risk appetite	'Risk appetite' is the amount of risk across a broad level that the Council is willing to accept in pursuit of objectives and value. 'Appetite'

	defines the Council's general approach to risk, and influences how risks are assessed and addressed, i.e. whether or not risks are taken, tolerated, retained, shared, reduced, or avoided, and whether or not risk treatments are implemented or postponed.
Risk criteria	Risk criteria are terms of reference and are used to evaluate the significance or importance of an organisation's risks. They are used to determine whether a specified level of risk is acceptable or not acceptable. Risk criteria should reflect your organisation's values, policies, and objectives, should be based on its external and internal context, should consider the views of stakeholders, and should be derived from standards, laws, policies, and other requirements.
Risk Evaluation	'Risk evaluation' is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or not acceptable.
Risk Level	The 'risk level' is its magnitude. It is estimated by considering and combining consequences and likelihoods. A level of risk can be assigned to a single risk or to a combination of risks.
Risk Management	'Risk management' refers to a coordinated set of activities and methods that is used to direct an organization and to control the range of risks that can affect its ability to achieve objectives.
Risk Management Framework	A set of components that support and sustain risk management throughout an organisation. There are two types of components: foundations and organizational arrangements: • Foundations include the risk management policy, objectives, mandate, and commitment. • Organisational arrangements include the plans, relationships, accountabilities, resources, processes, and activities used to manage the Council's risks.
Risk management policy	Defines a general commitment, direction, or intention. A risk management policy statement expresses an organization's commitment to risk management and clarifies its general direction or intention.
Risk management process	A risk management process is one that systematically applies management policies, procedures, and practices to a set of activities intended to establish the context, communicate and consult with stakeholders, and identify, analyse, evaluate, treat, monitor, and review risk.
Risk owner	A risk owner is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.
Risk profile	Is the written description of a set of risks relating to an entity. A risk profile can include the risks that the entire organisation must manage or only those that relates to a particular function or part of the organisation.
Risk source	A risk source has the intrinsic potential to give rise to risk. A risk source is where a risk originates, i.e. it is where the risk stems from.
Risk treatment	Risk treatment is a risk modification process, involving selecting and implementing one or more treatment options. Once a treatment has been implemented, it becomes a control or it modifies existing controls. The following risk treatment approaches, i.e. a '4T's':

	• **Treat:** to take one or more actions that could reduce the potential likelihood or impact or both of a risk occurring or to mitigate the effects of the risk should it manifest itself. • **Tolerate:** where the effects are likely to be within the identified risk tolerance, the Risk Owner can 'tolerate' the risk assuming they have the authority to do so. • **Transfer:** to move or transfer the effects of a risk to a third party, e.g. purchasing insurance, outsourcing, contractual transfers. • **Terminate:** to 'terminate' the action that gives rise to the risk, e.g. to stop a particular activity, to close down an operation or facility.
Stakeholder	A stakeholder is a person or an organization that can affect or be affected by a decision or an activity. Stakeholders also include those who have the perception that a decision or an activity can affect them. ISO 31000 distinguishes between external and internal stakeholders
Strategic Risk	Long-term threat or opportunity risk concerned with where the organisation wants to go, how it plans to get there and how it can ensure survival.
Target Level	The desired impact that a risk would have on an organisation if it occurred.
Uncertainty	Uncertainty (or lack of certainty) is a state or condition that involves a deficiency of information and leads to inadequate or incomplete knowledge or understanding