City of Greater Geraldton
a vibrant future

Risk Management Framework

2026 - 2028

Table of Contents

1 Introduction

The City of Greater Geraldton's (the City's) vision in the 2025-2035 Strategic Community Plan is Growing Greater Geraldton together. Our purpose is to create a strong, healthy and secure community through collaboration, partnership and good leadership. To fulfill our vision and purpose, we need to ensure that a systematic and structured approach to risk management is undertaken to effectively deal with the uncertainties in our mission.

Our Corporate Business Plan 2025 – 2029 outlines key areas of focus identified by our community:

1. Advocacy
2. Financial sustainability
3. Population growth
4. Climate and waste
5. Protecting the natural environment and greening suburbs
6. Housing
7. Community safety
8. Health services

This Risk Management Framework (the Framework) supports the City's Risk Management Policy (the Policy). This Framework sets out the City's processes and procedures for understanding, documenting, managing, and continuously improving risk management. The Policy outlines the City's commitment, appetite, tolerance, and approach to managing risks. This Framework supports and provides guidance to put the Policy into practice through integration of risk management in City activities and culture.

Effective risk management is essential to the City's operations and delivery of services to the community. Risk management requires sound corporate governance and integration of good risk management practice within processes, planning, reporting and performance measurement.
To ensure effective risk management is built into the City's culture, it must be built into everyday tasks and duties undertaken by staff. Risk management must be demonstrated in strategic planning and mandated in all operational functions and services.

The City's Risk Management Framework sits alongside a variety of other City frameworks, such as:

- Safety Management
- Human Resources
- Asset Management
- ICT Systems
- Emergency Management
- Compliance
- Financial Management
- Community Engagement
- Community Development
- Project Delivery
- Strategic Planning
- Statutory Planning
- Business Continuity

Effective leadership of risk management means that all staff understand the Framework and Policy and embed associated obligations in all operational activities.
The City has adopted the principles in the AS ISO Standard 31000:2018 Risk Management Guidelines (the Standard) with tailoring that suits City practice.

The Standard makes the following key statements:

- General (5.1) – the effectiveness of risk management will depend on its integration into the governance of the organisation, including decision-making. This requires support from stakeholders, particularly top management.
- Leadership and commitment (5.2) – top management and oversight bodies, where applicable, should ensure that risk management is integrated into all organisational activities and should demonstrate leadership and commitment by:
  - Customising and implementing all components of the framework
  - Issuing a statement or policy that establishes a risk management approach
  - Ensuring that the necessary resources are allocated to managing risk
  - Assigning authority, responsibility, and accountability at appropriate levels within the organisation.

The City implements these elements of leadership and commitment through:

- Submitting a Risk Management Framework and Risk Management Policy to the Audit, Risk and Improvement Committee and Council for endorsement to ensure it continually meets the needs of the organisation.
- Developing and maintaining a Business Continuity Management Policy which outlines the responsibilities of EMT and Managers with respect to Business Continuity Plans.
- Council endorsement of the operating budget includes internal audit and a business unit service of governance and risk mitigation advice, including employee resources.
- Assigns authority and responsibility for risk management through the development, endorsement, and implementation of the Framework.

2 Key Principles

Risk management needs to create and protect value. It must contribute to the achievement of objectives, improving performance, operations efficiency, increasing value for money, and promoting good governance. It is:

- Integrated into organisational processes: it is not a stand-alone activity and is a part of the City's planning and delivery processes.
- Structured and comprehensive: the approach to risk management must deliver consistent, comparable and reliable results which can be monitored and managed through standard templates and reporting mechanisms.
- Customised: customisation of each risk ensures that the optimum amount of risk management work is undertaken to support risk-based decision making.
- Inclusive: risks are discussed regularly and accepted as a necessary part of conducting business or actively managed to prevent or reduce the severity of disruptions or impacts to objectives. This includes timely escalation and involvement of relevant stakeholders.
- Dynamic: risk management should continually respond to change. As events occur, the context and knowledge change, monitoring and review of risks take place, new risks are identified and some may disappear. A system to deal with this in a proactive, iterative and responsible manner is essential.
- Based on best available information: resourcing of risk management is essential to ensure risks are based on experience, stakeholder feedback, observation, forward planning and expert judgment.
- Continually improved: risk management ensures the City continually makes informed choices, prioritises actions and plans strategically. Incidents and lessons learned inform strategies which are employed to continually inform the Framework and risk management practices.
- Continually taking human and cultural factors into account: the City recognises that differing capabilities, perceptions, and intentions of external stakeholders and staff can facilitate or hinder the achievement of objectives.

3 Governance

3.1 Three Lines of Defence

The City's Framework adopts a **Three Lines of Defence** operational model. This structured approach to risk management captures roles, responsibilities and accountabilities.

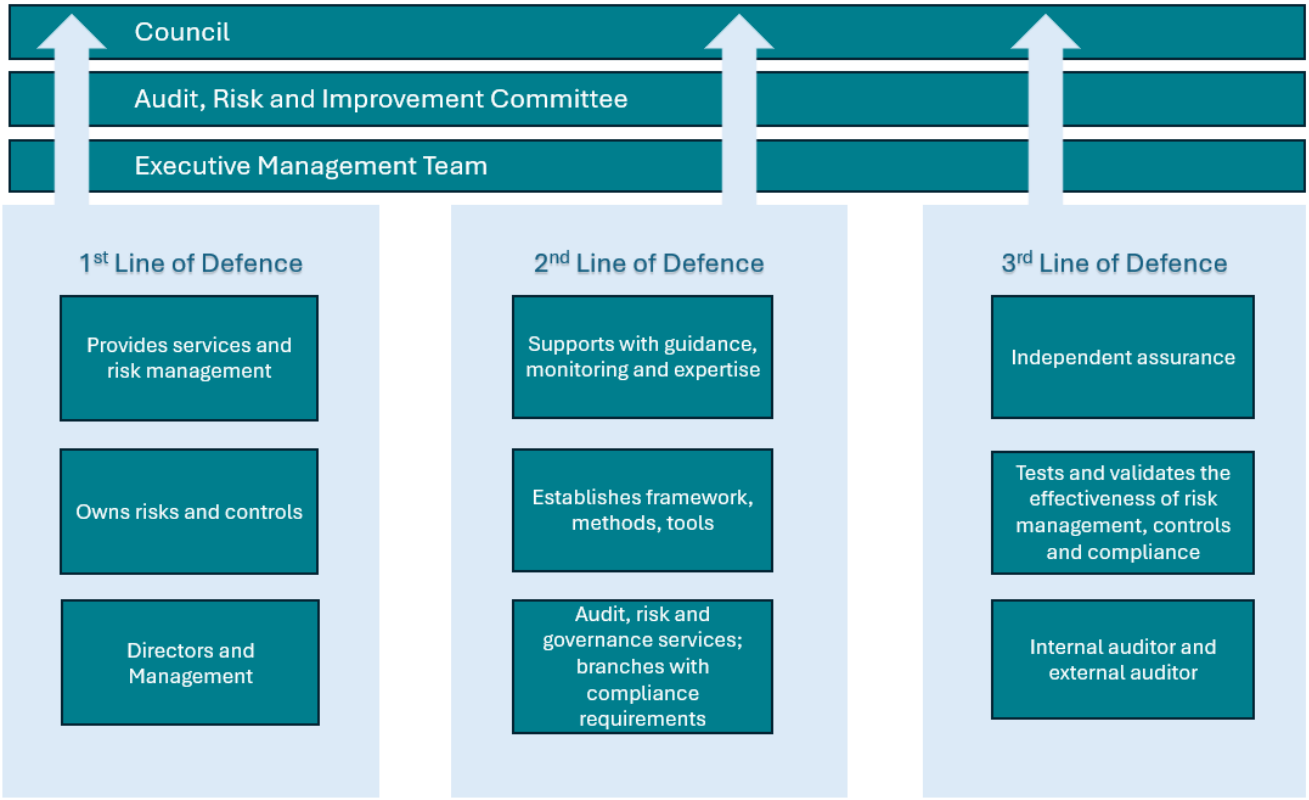
All lines of defence are responsible to provide assurance to the Chief Executive Officer (CEO), Executive Management Team (EMT) and Council (via the Audit, Risk and Improvement Committee (ARIC)) that risk is being managed at the highest level possible with available resources.

First Line of Defence: all operational areas are considered 1st line. It relates to those who are responsible for identifying and managing risk as part of their accountability in achieving objectives. They require the knowledge, skills, information, and authority to apply policies and procedures for risk control. An understanding of organisational objectives, the environment in which it operates, and the risks it faces is essential.

Second line of defence: Manager Corporate Compliance is responsible for providing the policies, frameworks, tools and support to enable risk and compliance to be managed in the first line. Support can also be obtained from other 1st line of defence teams which require compliance and contribute to risk control, for example, in the areas of finance, fraud and corruption, information technology and cybersecurity.

Third line of defence: is provided by internal audit and external audit and is independent of the first and second lines of defence. It ensures that the first two lines are operating effectively and advise improvements. Internal audits report to ARIC, providing evaluation through a risk-based approach, on the effectiveness of governance, risk management, and internal controls to the CEO, EMT, and Council. It also provides assurance of risk control in the achievement of objectives. The City's external auditors are the Office of the Auditor General (OAG) as appointed by legislation. The OAG are responsible for auditing all local governments in Western Australia.

Figure: Three Lines of Defence



3.2 Roles and Responsibilities

3.2.1 Council

Council is responsible for:

- Endorsing the Risk Management Policy and Risk Management Framework.
- Reviewing the appropriateness of risk tolerance.
- Receiving reports from the Audit, Risk and Improvement Committee in relation to risk management, internal control and legislative compliance as required by the Local Government (Audit) Regulations 1996.

3.2.2 Audit, Risk and Improvement Committee

ARIC is responsible for:

- Guiding and assisting the City in carrying out its functions:
  - under part 6: Financial Management, of the Local Government Act 1995.
  - in relation to audits conducted under Part 7 – Audit, of the Local Government Act 1995.
  - relating to other audits and other matters related to financial management.
- Reviewing the CEO's report into the appropriateness and effectiveness of the City's systems and procedures in relation to risk management, internal control and legislative compliance and report to the Council the results of that review.
- Considering the adequacy and effectiveness of internal controls by reviewing reports from the internal auditor, the administration, the OAG, consultants and other external oversight agencies as appropriate.
- Reviewing the Strategic and Major Project risks to the City and the plans to minimise or respond to those risks.

3.2.3 CEO

The CEO is responsible for:

- Leading and promoting a risk aware culture and taking appropriate action as required.
- Ensuring the identification and management of Strategic and Major Project risks.
- Ensuring establishment of a risk management process that is implemented and maintained in accordance with the Policy.
- Reporting outcomes of reviews undertaken at least once every four financial years to Council via the Audit, Risk and Improvement Committee on the appropriateness and effectiveness of the City's systems and procedures in relation to financial management, legislative compliance and risk management, presented to it by the CEO under regulation 17 of the Local Government (Audit) Regulations 1996.
- Presenting administrative reports to ARIC in relation to risk management, internal control and legislative compliance.

3.2.4 CEO and Directors (EMT)

EMT is responsible for:

- Promoting a positive risk culture.
- Ensuring inclusion of appropriate risk management in all planning activities.
- Managing the strategic and major project risk portfolio including raising new risks as they arise and ensuring mitigation strategies are appropriate and effective.
- Providing appropriate direction for reported risk (reporting frequency and accuracy) and associated control activities (effectiveness adequacy).

3.2.5 Directors and Managers

Directors and Managers are responsible for:

- Identifying, analysing and accepting risk on behalf of the City within the scope of services specified in their branch obligations.
- Providing leadership through a solid understanding of the City's Framework and Policy.
- Ensuring all planning activities use the City's risk documentation consistently and effectively.
- Monitoring use and effectiveness of risk management within their areas of responsibility including appropriateness of documentation and outcomes.
- Supporting attendance to risk-based training.

- Reviewing, updating and reporting risk for the Directorate unit specific plans alongside projects as required.
- Ensuring risks are reported and actioned appropriately.
- Maintaining and reviewing Business Continuity Management and Business Continuity Plans for their branches.

3.2.6 Manager Corporate Compliance

The Manager Corporate Compliance is responsible for:

- Reviewing the City's Framework and Policy, alongside feedback received from internal and external sources.
- Empowering management of risk through provision of guidance, tools and appropriate training.
- Undertaking risk maturity assessments to highlight areas of improvement.
- Managing strategic risk reporting to EMT
- Monitoring escalation of high and extreme risks for reporting to the EMT and Council (through the ARIC).
- Owning and promoting the Business Continuity Management Policy for the City.

3.2.7 Coordinator Governance and Risk

The Coordinator Governance and Risk is responsible for:

- Providing guidance on application of risk management processes.
- Administering the City's electronic risk management system for documenting risk.
- Providing advice on the quality of risk items documented.
- Developing and delivering risk training programs as part of the City's Induction Program and on request.
- Facilitating risk discussions as required.
- Providing input to the review of the City's risk management documentation and associated systems and processes.
- Coordinating risk reporting to the Manager Corporate Compliance.

3.2.8 Internal Auditor

The internal auditor is responsible for:

- Developing a risk-based internal audit program in conjunction with the CEO and Director Corporate Services.
- Completing internal audit reports detailing observations and making recommendations where appropriate, for risk mitigation and system improvements.
- Providing audit reports to the ARIC.

3.2.9 All Staff

All staff are responsible for:

- Attending risk training programs.
- Completing assigned risk actions.
- Reporting to management on risks that exist within their area.
- Performing duties safely and reporting hazards or incidents
- Making risk control and prevention a priority when undertaking tasks.
- Ensuring risk treatments and action plans are current and ensure all risk sign offs include evidence of compliance.

3.2.10 Project Managers

Project Managers are responsible for:

- Ensuring risk management for all projects is in accordance with the Project Delivery Framework in consultation with relevant stakeholders.
- Identifying, recording, and managing risks throughout the lifecycle of the project.
- Ensuring relevant risks are reported and escalated as necessary with the relevant stakeholders.
- Ensuring that reputational risks are managed in conjunction with Corporate Services.

4 Risk Management Process

Those with responsibility to accept risk on the City's behalf need to ensure that risks are managed in accordance with the responsibilities detailed in this Framework. They are responsible for ensuring the following steps are undertaken:

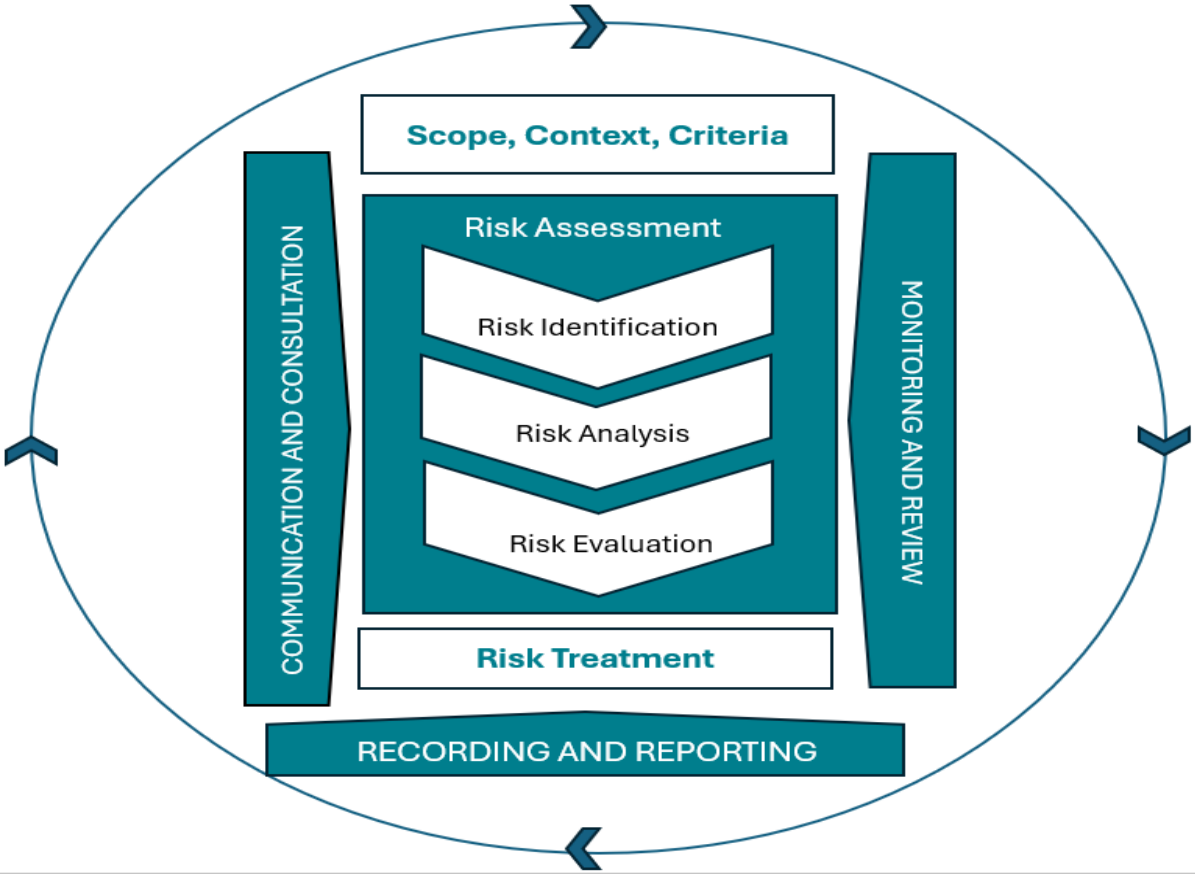
- Risks are identified and documented as required.
- Risks are to be reviewed at least quarterly for extreme and high risks, and at least six monthly for low and medium risk.
- Escalations are managed as early as possible and relevant issues reported to the EMT or responsible Director.
- Taking action to update risk information following publication of Risk Reports.

Support is available from Governance & Risk to assist teams in all aspects of risk management.

All planning activity is required to use the Risk Management Process and to document the outcomes and ongoing management using tools and templates that reference the organisational criteria, scope and context defined within this document.

The Risk Rating Matrix and Risk Assessment Process have been organised in sequential steps to reflect the risk assessment portion of the Risk Management Process.

Figure: Risk Management Process AS/NZS 31000:2018 Risk Management – Guidelines



5 Risk Management Process Steps

5.1 Organisational Criteria

The City sets criteria for risk management through the risk matrix. This includes a profile of risk classifications (key business areas of interest), risk levels, guidance on how to manage risks, risk appetite and associated required reporting.

The City's risk appetite is the willingness to take low and medium inherent risk without variation to existing control activities. High and extreme risks require deeper assessment of control performance and residual risk ratings to be provided for closer monitoring and improvement where possible or assurance of the highest levels of control performance at the current time.

All risk assessments must be documented using systems or tools that use the criteria referred to in the Risk Rating Matrix and Risk Assessment Process.

5.2 Risk Assessment

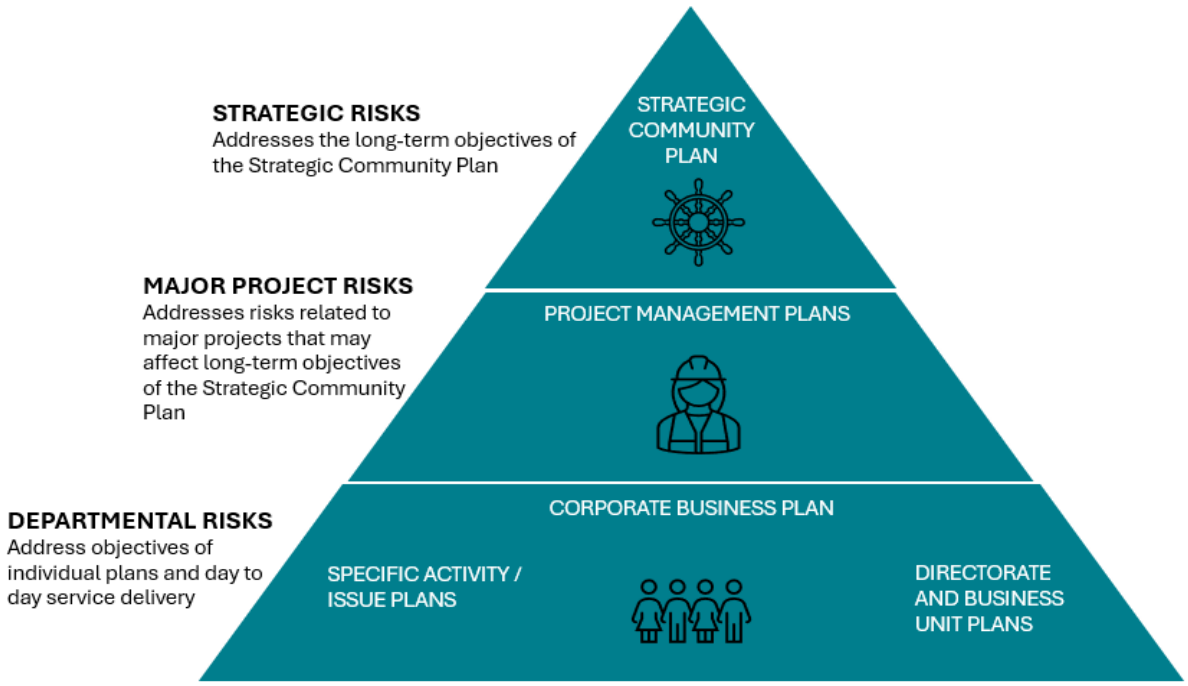
The City has identified three primary categories of risk that provide the scope and context of the risk assessment process.

The City uses the Promapp Nintex module to store, document, and report on the City's risks and treatments. All staff are responsible for ensuring that risks, treatments and signoffs are reported and current in Promapp.

Strategic Risk

Risks of an internal or external nature that affect the City's achievement of long-term objectives defined by the Strategic Community Plan and/or may have the ability to affect the whole of the City's operations.

This category is managed by EMT who are responsible for coordinating risk controls and their effectiveness and must be assigned to a Director for sign off.



Major Project Risks

A Major Project is a project that, due to its financial value, complexity, strategic importance, or potential impact on the community, environment, or organisational operations, requires enhanced governance, formal risk assessment, and elevated oversight beyond standard project management processes.

Major Project Risks are risks of an internal or external nature associated with the delivery of major projects which may affect achievement of long-term objectives defined by the Strategic Community Plan.

The degree of risk management effort and level of information captured is commensurate with the size, complexity, and inherent profile of the project. Major project risks are managed by the Project Sponsor with risk ownership and control coordinated by the Project Manager for the term of the project.

Departmental Risks

Risks of an internal or external nature that align to the delivery of operational activities defined within the Corporate Business Plan that delivers the vision outlined in the Strategic Community Plan.

Directors are named as Risk Managers to oversee risks of this nature at portfolio level to manage escalations. Managers are named as Risk Owners (except where employees have authority to accept risk directly to their role responsibility) to manage individual risks assigned to them by way of coordinating management of controls.

Managers are responsible for coordinating risk control and managing escalations in the absence of the Director.

Risk Identification, Analysis and Evaluation

Sources of risk (internal/external), areas of impact (classifications/profiles), causes, and potential consequences are identified to establish a list of risks that can enhance, prevent, degrade, accelerate or delay the achievement of objectives. Comprehensive identification is crucial – a risk not identified is not included in any analysis.

Methods of identification can vary and should include subject matter experts. A common approach for identification is brainstorming, which provides an array of results that can be further circulated to key stakeholders for input.

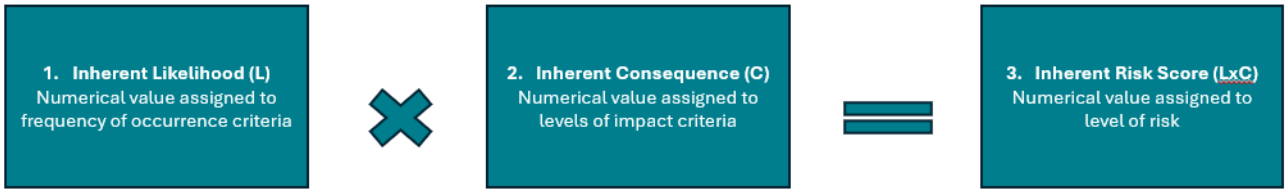
Basic questions that guide (not define) risk identification include:

- What can go wrong that will get in the way of objectives or goals? (risk event title)
- What will make it go wrong? (potential causes)
- What is the result if it does go wrong? (consequences)

Refer to Attachment 1 (Step 1) for Risk Rating Matrix and Risk Assessment Process.

How to provide a detailed risk description

How to rate inherent risk



Inherent risk is the risk level without considering controls and is determined using the values for consequence and likelihood in the Risk Rating Matrix and Risk Assessment Process (step 1 and step 2).

This is the worst foreseeable consequence (a judgment applied by subject matter experts) should controls with the possibility of failure all do so at the same time, however unlikely that may be.

Assigning a likelihood and consequence allows the associated values to be multiplied to give a risk score that aligns to a risk level.

Refer to Attachment 1 (Step 2) for Risk Rating Matrix and Risk Assessment Process.

How to rate residual risk

Control effectiveness is the review of control performance, both individually and collectively.

A control is an activity that positively influences risks it is assigned to. Control effectiveness levels need reporting for high and extreme residual risk. If a control has any chance of failing, meaning it doesn't consistently operate at the highest standard, then it cannot be counted as "fully effective" in the overall risk rating. Controls that do not meet this standard will be assessed for improvement. This might mean redesigning it, strengthening it, or replacing it.

Individual control effectiveness reflects how well a control achieves its intended purpose. It considers two things together:

- Design effectiveness – whether the control is well-designed to address the risk, and
- Operational effectiveness – whether it works reliably in practice.

It is an assessment by subject matter experts. It is not enough to say that a control exists or use the fact that it achieved milestones to indicate its success. There needs to be an assessment of how well it performed. Key performance indicators are useful to establish this.

Refer to Attachment 1 (Step 3) for Risk Rating Matrix and Risk Assessment Process.

Overall control effectiveness uses the percentage of controls that perform at the highest level to establish a rating. This provides an overall guide to the current risk management status when rating residual risk.

Refer to Attachment 1 (Step 4) for Risk Rating Matrix and Risk Assessment Process.

Operational sign off should only be undertaken by the person assigned to implement and monitor operational effectiveness. It is only this person that can understand if a control is operating as designed and is producing the desired result. Control sign off is reflective of operational functionality, not risk responsibility.

Evidence of effectiveness levels can be requested by Risk Managers or Risk Owners, EMT or Governance & Risk team.

Refer to Attachment 1 (Step 3 and 4) for Risk Rating Matrix and Risk Assessment Process.

Well-designed controls include response triggers to indicate where failures may exist when a process is:

- not performed the required number of times to be considered complete
- not conducted as documented without errors or components missed, regardless of the overall outcome

- completed outside of required timeframes for either statutory or internal service level compliance
- exposed to opportunities for misconduct or fraud/theft.

Operationally effective controls are those that can be identified – through evidence and/or discussion with individuals/groups that operate the control process – as meeting the points below:

- in place, in operation
- providing the same outcome at each operation
- having been inspected (observed or through evidence provided from operation)
- mitigate cause and/or likelihood factors of risks they are assigned to

It is difficult to have a single control that meets all the design and operational effectiveness elements. Risk Managers should ensure that collectively these are covered for risks they are responsible for.

Risk Treatments are plans to implement change in the risk and/or control environment, that is to reduce causes and/or likelihood of a risk event occurring. These should be balanced with the cost and efforts of implementation against the benefits derived.

Treatment plans are required where residual risk remains as high or extreme or where it has been requested by the Risk Manager or Risk Owner, to improve or replace existing controls.

Subject matter expert judgment should always be used to determine where further action is required.

5.3 Communication and Consultation

Effective communication and consultation are essential to ensure that those responsible for managing risk, and those with a vested interest, understand the basis on which decisions are made and why particular treatment / action options are selected or the reasons to accept risks have changed.

5.4 Monitoring and Review

It is essential to monitor and review the management of risks as changing circumstances may result in risks increasing or decreasing in significance. It also ensures that new risks are identified as appropriate.

Additional monitoring and review are undertaken as part of the Internal Audit Plan and control audits that are implemented by Corporate Services.

Refer to Attachment 1 (Step 6) for Risk Rating Matrix and Risk Assessment Process.

5.5 Risk reporting

All risks are maintained within 'Promapp'. This allows the centralised reporting function to meet the City's requirement to monitor and review risks by all levels of management, the Audit, Risk and Improvement Committee, and Council.

Formal reporting is provided as follows:

- Quarterly reporting to EMT or as required (those risks with a residual rating of high, extreme or medium)
- Quarterly Risk Report of Strategic and Major Project risks to the Audit, Risk and Improvement Committee
- Annual Risk Report to Council
- Risk Escalation Reports

Refer to Attachment 1 (Step 6) for Risk Rating Matrix and Risk Assessment Process.

To ensure reporting is relevant, Risk Owners are responsible for ensuring:

- New/emerging risks for all risk categories are identified, continually managed and escalated as required to the Director or EMT
- Operational risk portfolios are up to date and reflective of services delivered, objectives and current risk environment.
- Project risks are managed and reported appropriately.
- Controls and their effectiveness are monitored and updated, escalating any significant issues to the Director or EMT.

- Escalations (overdue, non-compliant, reportable risk, risk reviews) are managed in a timely manner.
- Timely response to risk notifications from the City's electronic risk management system and from Governance & Risk.

Directors are responsible for ensuring (both in their role as Director and EMT member):

- Identification and management of a relevant strategic risk portfolio and associated control activity as part of the EMT role.
- Provision of direction on reporting frequency and agreement to the highest control effectiveness possible for risks that do not meet the risk appetite.
- Managing escalations for any category of risk appropriately.
- Formal risk reviews are conducted within required timeframes or at the time of significant change to the risk environment (restructure, risk ownership changes, external environment change).
- Responding to risk notifications from the City's electronic risk management system and from Governance & Risk.

6 Risk Matrix

Step 1: Profile your risk consequences against each classification. Note: not all criteria for each consequence may apply, choose what best fits the situation being assessed.

CONSEQUENCE	Health, Safety & Wellbeing	Financial Loss	Service Delivery	Reputation	Environment	Legal and Compliance
INSIGNIFICANT (1) Little or no effect on objectives	Temporary situation, resolved in easy to manage timeframe, acceptable increase in incidents, absence & liability claims. 3 days – 3 weeks	Less than $10,000 Dept./Project 0-2% remaining budget.	Temporary delays, easily cleared backlog/customer requests increase. 1-7 days	Minor news/media impact, normal levels of complaints, easily resolved issue, minimal impact to staff turnover.	Contained reversible damage using existing resources.	Easily resolvable breach, most objectives will be met, internal systems identify potential fraud or corruption incidents.
MINOR (2) Effects are noticeable but not critical to objectives	Not permanent, formally registered incident, manageable recovery timeframe, increase in incidents, absence & liability claims manageable. 1 month – 3 months	Organisation less than $250,000 Dept./Project 2-5% remaining budget	Some key deliverables delayed, some program delay/cancellation, manageable disruption daily, customer request increase and missed targets/non-conformances manageable. 2-4 weeks	Substantiated issue, public embarrassment, manageable news/media profile, possible internal investigation, manageable impact to staff turnover.	Clean-up required, additional resources may be required, external agency involvement.	Breach requiring internal investigation and/or unplanned audit, use of reactive risk controls/damage control, overall compliance may drop, some objectives will not be met.
MODERATE (3) Serious impact to the course of action or objectives	Extensive impairment/injury, medical intervention/hospitalisation, partial/full recovery, increase in incidents, absence & liability claims higher than projected/requires resources to manage. 4 months - 12 months	Organisation $250,000 - $1M Dept./Project 15-20% remaining budget	Routine activity cancellation, daily monitoring by senior staff, prolonged interruption, requires additional resources, customer request increase and missed targets/non-conformances need active management. 4 – 12 weeks	Day to day disruption, local news/media profile, effort and expense required, internal and/or external investigation, staff turnover increase requiring additional resources to manage.	Uncontained, major but recoverable contamination, coordinated response from external agencies, significant resources required.	Breach requiring external investigation, rectification or termination may be required, audit plan delayed, risks require treatment, low compliance, objectives rarely met, opportunity for fraud or corruption not managed, ineffective process not picked up.
MAJOR (4) Extensive and critical impact to the course of action or objectives	Loss of life, permanent/injury impairment, ongoing situation, external investigation, extended resources required to manage, unmanageable liability claims, fraud or corruption impacts including imprisonment, personal fines, employment termination/s or losses, liability claims.	Organisation – > $1m Dept./Project greater than 20% remaining budget	Cancellations, activities terminated, immediate intervention required, significant service changes required, fraud or corruption-based delay including poor process management.	Widespread multiple news/media profile, significant damage requiring external investigation and intervention, including fraud or corruption. Staff turnover not manageable without service impacts including turnover related to fraud or corruption incidents.	Uncontained, extensive contamination, potentially irreversible. External intervention and considerable resources required to manage, any environmental impacts related to fraud or corruption incidents.	Breach requiring external investigation and action, audit plan will not be completed significant loss, risks impact increases, unable to meet required compliance or objectives, fraud or corruption incidents committed that are internally or externally reported, wide-spread fraud or corruption incidents.

Step 2: Determine the likelihood and multiply it against the consequence for each classification from step 1. This provides a risk profile. The highest risk value is the risk rating.

CONSEQUENCE	LIKELIHOOD DESCRIPTORS		
	UNLIKELY (1) Risk is unlikely to occur	POSSIBLE (2) Risk could occur, but not certain	LIKELY (3) Risk is likely to occur
INSIGNIFICANT (1) Little or no effect on objectives	LOW (1)	LOW (2)	MEDIUM (3)
MINOR (2) Effects are noticeable but not critical to objectives	LOW (2)	MEDIUM (4)	HIGH (6)
MODERATE (3) Serious impact to the course of action or objectives	MEDIUM (3)	HIGH (6)	HIGH (9)
MAJOR (4) Extensive and critical impact to the course of action or objectives	MEDIUM (4)	HIGH (8)	EXTREME (12)

Step 3: Identify controls (activities managing consequences or likelihood) for each risk and establish individual performance. Evidence may be asked for.

INDIVIDUAL CONTROL EFFECTIVENESS (apply to each control)	Individual control criteria/guidance
Control operates mostly as intended, MEETS its own objectives (Only controls at this level apply in step 4)	Control is mostly well designed (meets most of the response triggers that indicate when things go wrong, such as not performed the required number of times, if forgotten or lost, if completed within required timeframes (statutory or internal), if performed as designed regardless of the outcome and can protect against misconduct/fraud both internal and external). It is operationally effective i.e. it is in place, is a repeatable process that provides the same outcome, has been inspected (observed or through evidence), works to mitigate risk (it is managing cause/s and/or likelihood factors).
Control operates well but DOES NOT ALWAYS meet its own objectives	Control design and operational effectiveness is sometimes satisfactory but can be improved, works to mitigate elements of risk.
Control does not always operate well, often NEEDS IMPROVEMENT to meet its own objectives	Control design and operational effectiveness is not that good, should be improved, works to mitigate a few elements of risk.
Control rarely operates well or is not fully implemented, DOES NOT MEET its own objectives	Design and/or operational effectiveness is not allowing control to mitigate significant elements of risk. If this cannot be changed, consider treatment plans to improve overall effectiveness and/or replace poorly performing controls.
Control not measured for effectiveness OR treatment has not yet been implemented	Measure design and effectiveness of control as soon as possible to ensure this control contributes to overall effectiveness levels. Treatments that are being implemented should assess effectiveness as soon as any results can be determined, even if they will improve over time.

Step 4: Allocate an overall control effectiveness rating by assessing the % of controls performing at the highest level from step 3

OVERALL CONTROL EFFECTIVENESS RATING	% of controls that operate mostly as intended, MEETS its own objectives
STRONG	>75% to 100%
ADEQUATE	>50% to 75%
DEVELOPING	>25% to 50%
INADEQUATE	0% to 25%

Step 5: Rate the residual risk by repeating step 2 and 3 for the classification with the highest risk level considering step 3 and step 4

Step 6: Monitor, review and report – reviews changes in context, likelihood, consequence, effectiveness, residual risk and overall risk environment

INHERENT RISK LEVELS	Guidance to manage	Reporting	Review	Responsibility
LOW (1-2)	MONITOR WITH DAY-TO-DAY OPERATIONS by Risk Owners; adequate and/or partially effective controls acceptable; consider if all controls are required.	No formal reporting required, included in Monthly Risk Report published internally for risk responsible officers to review.	At least annually or when change occurs	Operational Managers
MEDIUM (3-5)				
HIGH (6-9)	MONITORING REQUIRED by EMT to ensure highest control effectiveness possible is being applied and reasonable efforts to investigate treatment plans are undertaken.	Governance & Risk to provide Quarterly Risk Report to EMT and Audit, Risk and Improvement Committee for review.	Quarterly unless otherwise directed, or when change occurs	Directors, EMT and CEO
EXTREME (10-12)				CEO and Council