RISK MANAGEMENT FRAMEWORK

Date adopted by Council: 25 October 2023

RISK MANAGEMENT FRAMEWORK

TABLE OF CONTENTS

PART 1 - INTRODUCTION

Organisations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives. Managing risk is an integral part of good governance and leadership and is fundamental to how an organisation is managed at all levels.

Importantly, risk management is an iterative process that supports organisations in setting strategy, achieving objectives and making informed decisions. It is part of all activities associated with an organisation and considers both the external and internal context of an organisation, including human behaviour and cultural factors.

STATEMENT OF COMMITMENT

Colac Otway Shire Council (Council) is committed to managing risks that challenge its ability to meet its strategic objectives and obligations to the community. Council will do this by logically and systematically identifying, minimising, managing, monitoring and communicating all risks that directly or indirectly influence Council's ability to achieve the vision and strategic objectives outlined in the Council Plan.

Council will make informed decisions on activities that it undertakes by appropriately considering risk and will work in cooperation and consultation with employees (and others involved with our activities and facilities) to ensure the achievement of Council objectives.

Council will strive to ensure that it does not place the community, employees, visitors or contractors at risk of harm to their reputation.

PURPOSE

To formalise and document Council's commitment to an enterprise wide risk management program that identifies, manages and minimises Council's risks in the achievement of Council objectives.

SCOPE

This Framework:

- Applies to all Councillors, employees, volunteers, contractors and partners.
- Establishes the guidelines for Council to implement effective risk management.
- Outlines various roles and responsibilities required to manage risk.
- Outlines governance requirements to ensure the framework, procedures, and tools remain compliant and effective.

OBJECTIVES AND OUTCOMES

The objectives of this Framework are to:

- Provide a structured, consistent and documented framework to guide Councillors, employees, contractors and volunteers in undertaking risk management activities.
- Drive a proactive risk management culture where awareness, engagement, assessment and mitigation of risk is embedded in all decision-making processes.
- Clearly define Council's risk attitude and risk tolerance levels to ensure alignment with business objectives.
- Ensure accountability for risk management at all levels of the organisation through measurable KPI's based on quality data.
- Ensure continual improvement in relation to risk management through regular review of people, processes, and systems to achieve best practice and ensure measurement and evaluation.
- Ensure measurement and evaluation of risk management practices.

TERMS AND DEFINITIONS

Key Terms and Definitions are listed in Appendix 1.

RISK MANAGEMENT PRINCIPLES

Effective risk management creates and protects value, improves performance, encourages innovation and supports the achievement of objectives.

Council maximises the effectiveness of risk management through compliance with the following principles:

- **Risk Management creates and protects value:** demonstrable achievement of objectives and improvement in our risk performance.
- **Risk Management is an integral part of processes:** demonstrating that management responsibility includes the accountability for risk management and its integration with our processes.
- **Risk Management is part of decision-making:** demonstrating that risk management underpins our decision-making resulting in informed choices, prioritised actions and development of alternative courses of action.
- **Risk Management deals with uncertainty:** demonstrating that our processes, activities and decision-making address uncertainty.
- **Risk Management is systematic, structured and timely:** demonstrable consistent, comparable and reliable achievements in efficiency.

- **Risk Management i**s based on best available information: demonstrating that the process of managing risk is based on data, experience, feedback, forecasts and consider the possible limitations of these information sources.
- **Risk Management** is tailored: processes that take into account the consideration of our risk profile.
- **Human and Cultural Factors:** processes accounting for the capabilities, perceptions and intention of employees and the community that may enhance or hinder our objectives.
- **Transparent and Inclusive Processes:** involving our decision makers, internal and external stakeholders when appropriate to ensure that our risk management is relevant and up-to-date.
- **Dynamic and Responsive Processes:** risk management processes designed to monitor, sense and respond to change resulting from changes in internal and external events and knowledge.
- **Continued Improvement of our Organisation:** recognising the need to develop and implement strategies to improve our risk management performance.

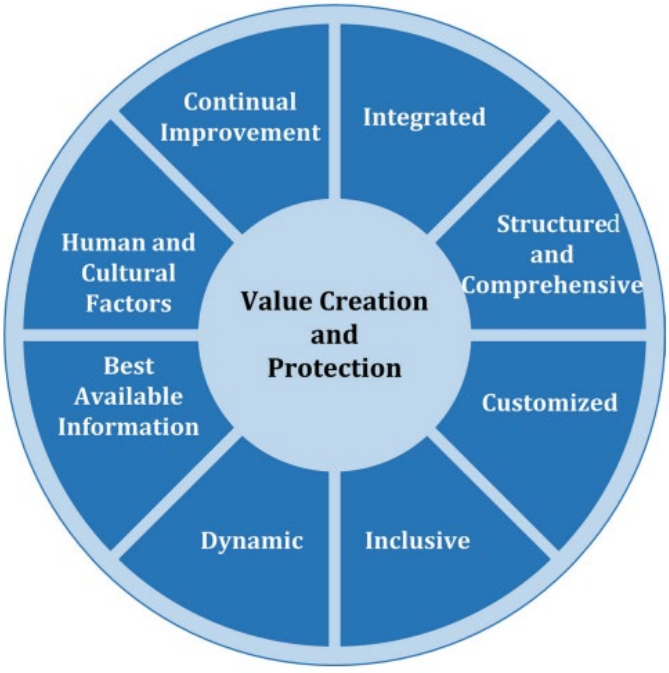


Figure 1 - Principles

PART 2 – INTEGRATION OF RISK INTO COUNCIL ACTIVITIES

The Australian Standard ISO 31000:2018 provides that the components of an effective Framework are:

1. Leadership and commitment
2. Integration
3. Design
4. Implementation
5. Evaluation
6. Improvement.

These are explored in more detail in following sections.

LEADERSHIP AND COMMITMENT

The principal strategy for managing risk throughout the organisation is to apply and integrate the risk management framework across all operations, with a view to proactively identify and quantify risks in order to develop effective treatment/control measures.

By implementing the risk methodology into everyday practice, embedded in the culture and mindset rather than processes alone, then a mature organisation will have the confidence to accept certain risks.

Risk leadership, ethics and culture for Council will be fostered through the discussion and communication of risk across all levels. To facilitate this, a common understanding of Council's risk management practices will be developed by discussing risk during decision-making and the provision of risk training where it is required.

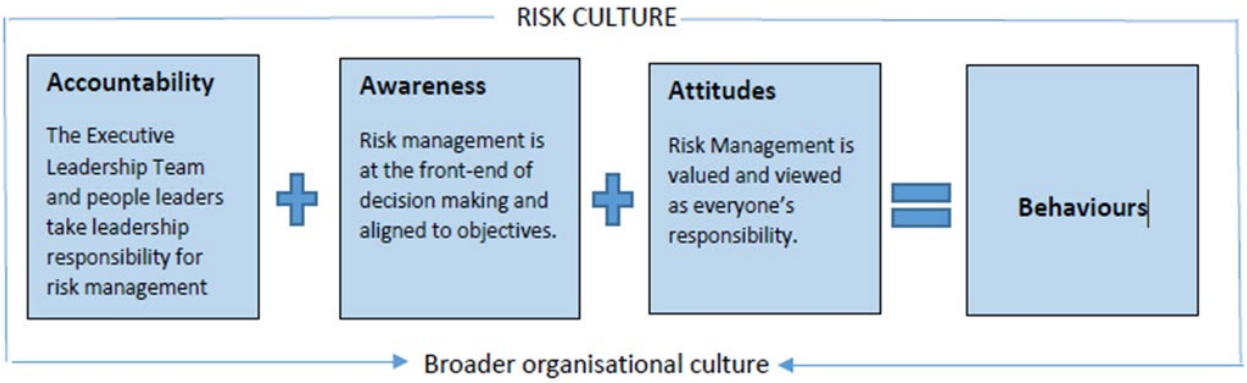
Council and the Executive Management Team will demonstrate leadership and commitment by:

- Developing, implementing and monitoring the Risk Management Framework that establishes the risk management approach to be taken by the organisation.
- Ensuring that the necessary resources are allocated to managing risk.
- Emphasising that risk management is a core responsibility.
- Assigning authority, responsibility and accountability at appropriate levels within the organisation.

Risk Culture

Council's risk culture does not sit separately or alongside the organisational culture. It is a component of the organisational culture that illustrates how risk awareness, accountability and attitudes are applied at Colac Otway Shire.

Embedding risk behaviour into process mechanisms leads to a sustainable risk culture. It enables us to confidently perform daily operations and make informed decisions knowing that the risks impacting our work have been rigorously assessed and appropriately mitigated.



Source: Victoria Government Risk Management Framework Practice Notes – Risk Culture

However, with changes in strategic direction, organisational priorities, funding availability and inevitable turnover of employees, risk values and capability can often be eroded. To mitigate this risk, Council's approach is to embed risk culture into the mechanisms of our operating environment to help ensure risk behaviours are repeated, sustained and positively impact our organisation and community.

Risk culture at Colac Otway Shire is evident through our:

- Councillor and Employee Codes of Conduct
- Officers' adherence to their delegated authorities
- Organisational values evidenced through behaviours
- Induction and training programs
- Position descriptions
- Regular performance reviews
- Risk profiling and participation
- Audit programs
- Risk recording and reporting.

INTEGRATION, DESIGN AND IMPLEMENTATION OF THE FRAMEWORK

In an integrated risk management framework, risk management activities and practices are incorporated into the everyday business as usual activities. These practices work in conjunction with Council's policies, values and culture. The intention is not to "bolt on" risk considerations to existing processes, but to blend in risk considerations in a way that risk is part of the business as usual (BAU) processes, and is a value add or can assist to prevent value destruction.

There is an organisation-wide responsibility for managing risk, and integrating risk management into an organisation is a dynamic and iterative process. Risk management should be a part of Council's purpose, governance, leadership and commitment, strategy, objectives and operations.

Organisational context

When designing a framework for managing risk, it is important to evaluate and understand the external and internal context. Colac Otway Shire's external context includes social, cultural, political, legal, regulatory, financial, technological, economic drivers and trends that impact objectives and relationships with, and perceptions and values of external stakeholders.

Council establishes internal communication and reporting mechanisms to support and encourage accountability and ownership of risk.

DESIGN

This Framework considers, amongst other things, Council's role in the community, its obligations, objectives and business processes, to create a Framework that is tailored to suit Council's needs and operating environment (it is fit for purpose). As demonstrated in this document, the Framework has assigned roles accountabilities and resources for risk management and the channels for risk consultation are described in separate Risk Procedures.

IMPLEMENTATION

The aim is to fully embed the risk management process in the organisation's critical processes and business processes so that it is as relevant, effective and sustainable as possible. This includes linking and integrating risk management with Council's business planning cycle and Improvement and Program Integration reviews and methodology.

Business Plans are four-year strategies for each work area that are revised annually and in line with the four-year Council Plan. Business planning involves formally reviewing and planning for services and ensures that work area activities are consistent with the strategic direction.

In order to have effective business planning, it is essential for departments to consider and review risks relating to their Business Plan. This maximises the chances that opportunities are realised and Business Plan actions will be completed as planned and on time. Stand-alone projects, events or activities that arise during a year should also be assessed for risks as they are planned. Setting the scope and boundaries of the risk management process involves:

- Defining the project or activity and establishing its goals and objectives.
- Defining the extent of the project.
- Identifying any studies needed.
- Defining the extent of the risk management activities to be carried out.

The Standards covering AS ISO 31000 Risk Management; OH&S Management Systems, AS4801 including Quality Management and AS/NZS 4804; Environmental Management, AS/NZS ISO14001 and AS/NZS 4581 Integrated Management Systems are some relevant references that assist in integrating risk management.

EVALUATION

Risk management performance is assessed through feedback on:

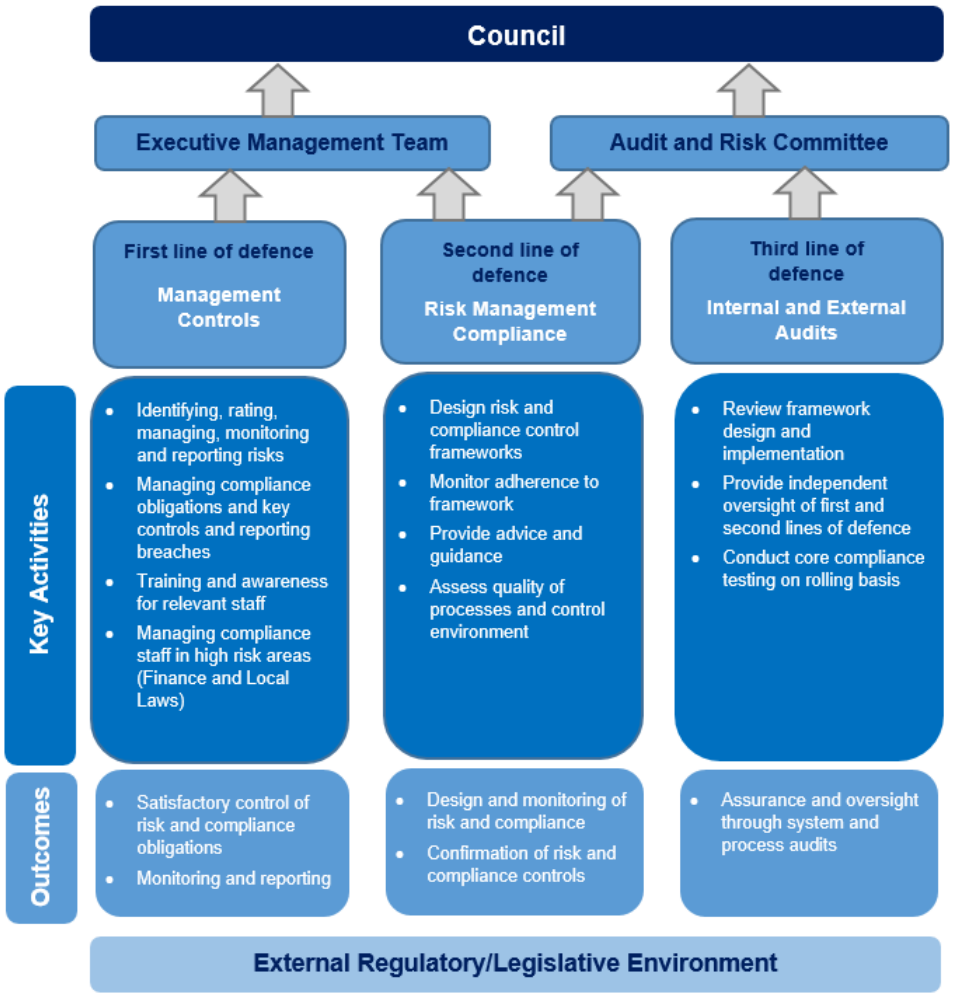
- The design, execution and outcomes of risk profiling and reporting activities.
- Implementation of risk tools into the business as usual activities.
- People and Culture performance management in accordance with Council's Risk Appetite.

IMPROVEMENT

The Framework and associated components are reviewed on a periodic basis to ensure they remain current, reflect better practices and are fit for purpose.

ASSURANCE

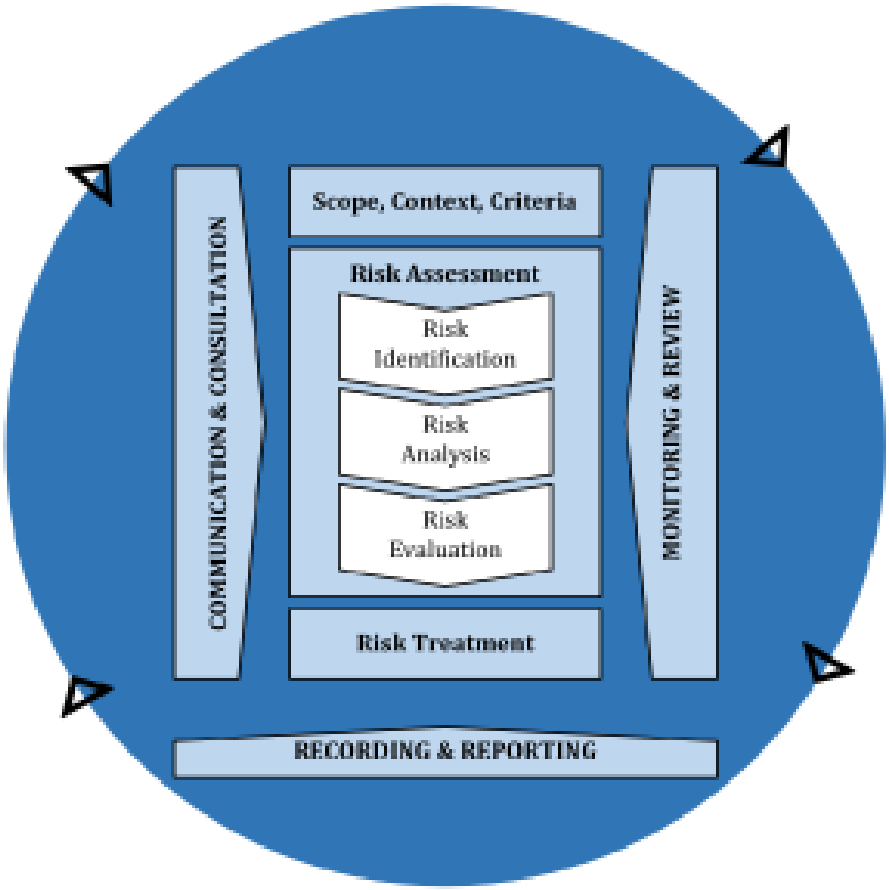
The three lines of defence assurance model represents Council's governance oversight for the risk management framework.



PART 3 – RISK MANAGEMENT PROCESS

The risk management process involves establishing the context, assessing, treating, monitoring, reviewing, recording and reporting risk. The risk management process methodology is consistent with Australian Standard ISO 31000:2018.

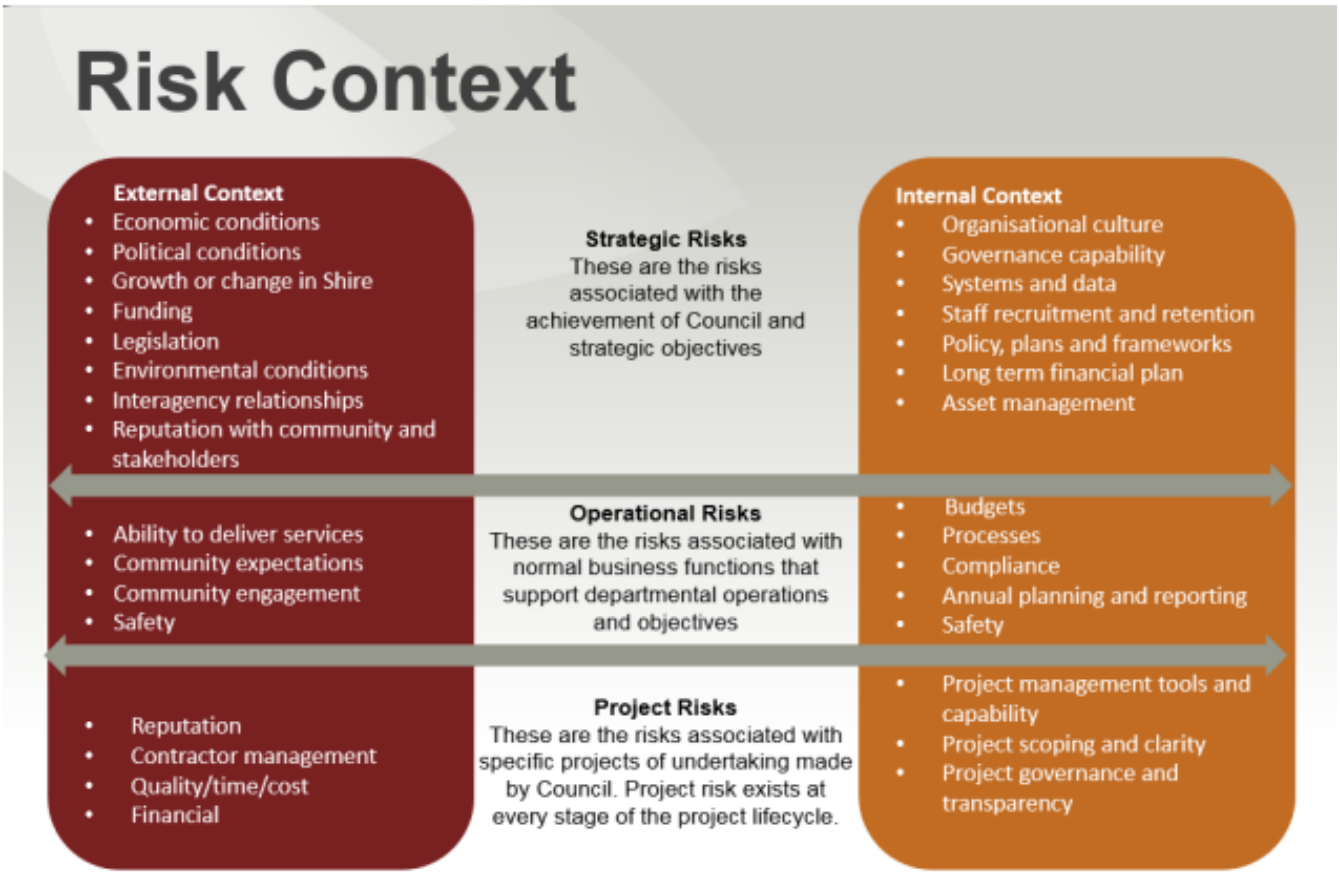
Figure 5 – Process



SCOPE, CONTEXT AND CRITERIA

The context in which the organisation assesses risk should be established prior to commencing a risk assessment. Establishing the context requires an examination of the external, organisational and risk management environment in which the risk identification, analysis and treatment options will be considered. This assists in establishing the assessment criteria for risk and the structure of the analysis.

Figure 6 – Risk Context



RISK APPETITE

Risk appetite represents how much risk Council is willing to take on to achieve its strategies and objectives. Risk appetite statements are a shared understanding of what is acceptable and unacceptable risk taking in each of the areas of Council's business. These statements help to avoid personal perceptions and biases that can adversely influence risk based decisions.

The following risk appetite statements have been developed with Councillors.

Risk Category	Category Description	Appetite Statement
Safety	Risks relating to managing the physical and general work environment and Council controlled spaces and their impact on health and safety of employees, contractors, volunteers or members of the public.	Council has no appetite for work practices, actions or inactions that compromise the wellbeing and safety of people including employees, contractors, volunteers and community.
Financial	Risks associated with the financial management of Council and its ability to fund Council services now and into the future (including risks related to revenue, expenditure, budget management, investments and debt management and accuracy of financial information).	Council has a small to medium appetite for variation in financial performance as long as long-term financial sustainability is not threatened.
Cyber Security	Risks relating to the security of the network, applications and information security and disaster recovery.	Council has a no appetite for external and internal threats, misuse, modification and unintended damage to the security of its ICT systems/environment.
Reputation	Risks relating to negative stakeholder opinion or negative publicity regarding business practices, Council decisions or behaviour of officers and Councillors.	Council understands that negative publicity may occur where there is competing priorities and interests in the community. Council has a medium to large appetite for impacts on Council's reputation.
Asset Management	Risks arising from the potential deterioration, damage or destruction of Council assets and road infrastructure (including both financial costs of repair and/or replacement and the impact that loss of access to the asset has on service delivery).	Council has no appetite to compromise on standards that impact on public safety. Council has a small to medium appetite and will accept some level of risk over non-core or non-essential assets and infrastructure.
Environmental Impact	Risks associated with Council's operations that have potential or actual negative environmental, ecological or cultural heritage impacts, regardless of whether these are reversible or irreversible in nature.	Council has a small appetite for risks that cause significant and irreparable damage to the environment and seeks to preserve and enhance it for future generations.
Governance	Risks relating to regulatory obligations and expectations and good governance framework and principles.	Council has small appetite for breaches of legal obligations, good governance principles, policies or contractual agreements that result in fines, penalties or reputational damage. Council has zero tolerance for illegal activities including fraud and corruption.

RISK ASSESSMENT

Step 1 – Risk identification

Identification of risks is a systematic determination of what, how, where and when an event may happen that could affect Council's day-to-day operations.

Risks can be identified by looking at historical performance and trends, previous events, current challenges, and the needs of those who use our services, as well as thinking about future scenarios or potential outcomes that could prevent us from providing safe and sustainable services and hinder the delivery of our long-term strategic objectives.

Risks may be articulated using the following method to provide for clarity and brevity:

EVENT: what will happen?

CAUSE: why the event could happen?

IMPACT: how bad will it be if it did happen, what is the exposure to Council?

Step 2 – Risk analysis

Once a risk has been identified, the controls currently in place must also be identified. Controls are mechanisms or processes that eliminate or reduce the impact and/or likelihood of the risk, include but are not limited to:

- Policies
- Procedures
- Training schedules
- Manuals
- Guidelines
- Audit
- External reviews
- Business continuity plans.

Step 3 – Risk evaluation

Risks identified are rated according to the likelihood of them eventuating and the consequence(s) that might flow if they did eventuate. This rating determines the level of risk exposure, urgency and complexity of treatment, and escalation processes.

Likelihood (How Often)

- The first step in determining the rating of the identified risk is to evaluate the likelihood of it occurring.
- The Likelihood Matrix included in the Risk Assessment Matrix at Appendix 2 is used to assess how probable it is that a risk will occur on a scale of 1 to 5, with 1 indicating it will happen rarely, and 5 indicating that it is almost certain to occur.

It is important to note that this score is arrived at using the expertise, knowledge and experience of the individual and/or group scoring it. This will often be the risk owner and/or risk champion.

Likelihood scoring may be challenged by the Risk and Insurance Officer, EMT, your direct supervisor or the Audit and Risk Committee reviewing the risk registers.

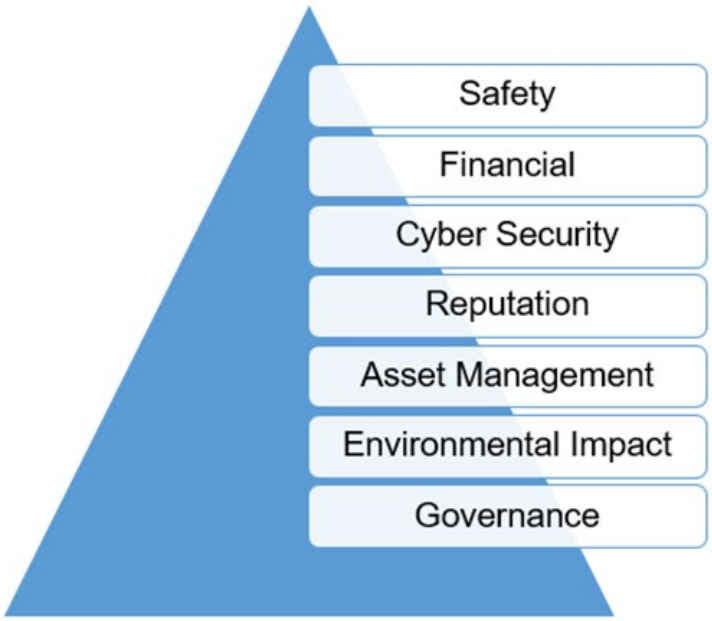
When adding a risk to the risk register, likelihood is determined during three stages:

- the first is the inherent rating without the current controls in place, or very weak controls in place;
- the second is the residual rating with the existing controls that are in place; and
- the third is when projecting the target risk rating.

Generally, the higher the degree of effective controls in place, the lower the likelihood score.

Consequence (How Bad)

Having assessed the likelihood, the second part of the evaluation identifies what the potential consequences or impact of the risk might be. The Risk Assessment Matrix at Appendix 2 categorises the areas of risk particular to Council's activities:



The consequence table rates the impact of a risk from 1 to 5, with 1 being insignificant or negligible impact and 5 being catastrophic.

Because the nature of risk is anticipating what may happen, the Consequence Table provides non-exhaustive examples of the impact of risk within a range. However, as with the scoring of the likelihood of a risk occurring, subject matter experts within that category of risk are evaluating the score and as such are able to anticipate an impact taking into account historical performance and trends, previous events and current challenges.

Risk Rating

Once the likelihood and consequence ratings have been arrived at they are multiplied to reach a risk rating, using the 5 x 5 matrix ("Risk Rating Matrix") at Appendix 3. This acts as a heat map to assess the severity of individual risks, determine Council's tolerance of it and drives the complexity and urgency of treatment approaches and escalations.

Where a rating is in the high to extreme end of the heat map, there is likely to be both more complex and urgent mitigations and action plans required, and it is escalated up the reporting line so that senior leaders are aware and are able to keep an eye on the way the risk is being managed. However, a medium risk will be treated at the local level i.e. Council is confident that there are processes and management structures in place to deal with the risk.

Council's risk registers require an evaluation of risk using the 5 x 5 matrix in 3 stages, without controls in place/weak controls in place (inherent rating), with the current controls in place (residual rating), and a target or projected rating.

RISK TREATMENT

If controls are not in place, or not working effectively, action plans may need to be developed to strengthen the control and manage the risk. Keeping in mind the balance between costs to implement the treatment versus the benefit to Council, the following treatment options may be considered:

- **Mitigate or reduce the risk:** This seeks to reduce the likelihood and/or impact of the risk by taking early action to reduce its occurrence to an acceptable level, and is the most common treatment action at Council.
- **Avoid the risk:** Decide not to proceed with the activity likely to generate the risk where this is practical.
- **Transfer the risk:** May be appropriate where another party can take on some or all of the risk more economically or more effectively i.e. a contractor or insurer, who may be better placed to manage the risk. Close review is required on transfer as it does not eliminate the risk altogether, but gives another party responsibility for its management.
- **Accept the risk:** By accepting a risk this does not imply it is insignificant. Acceptance may be an option where action is out of Council's control, or the risk is at an acceptable level within Council's risk appetite and tolerance levels.

Treatment plans may include the development or redesign of systems or policies and procedures; training and education; supervision; audits; and technical controls.

MONITOR AND REVIEW, COMMUNICATE AND CONSULT

The processes of monitor and review, and communicate and consult bookend the risk management process. They are dealt with together in this section as there is interplay between the two throughout the assessment process, as well as the framework generally.

Review of Risk Registers

- A continual process of monitor, review and improvement of all components of the Risk Management process is required to ensure risk registers are effective and current. During these reviews the residual risk rating will be reviewed and assurance sought on the delivery of action plans, their effectiveness and impact on the risk rating.
- For operational risks, risk champions, along with the risk owners, are responsible for the periodic risk reviews and for facilitating risk discussions at team meetings, committees and the overall management of the operational risks for their department. Timing and responsibilities are dependent on the level of risk. The higher the risk rating the closer monitoring is required.
- Operational risk reports should be discussed with General Managers on a regular basis (dependant on residual risk rating) to determine whether escalation is required or further action is to be taken. Where further information or clarification is required it is the responsibility of the risk owner to facilitate this.
- Strategic risks are reviewed by EMT on a rotational basis and reported to the Audit and Risk Committee biannually.

RISK MATURITY

Risk maturity is not a static concept. Over time the working environment changes, and risk management also needs to evolve to ensure it continues to support Council in achieving its objectives.

Risk maturity goes beyond the structural elements of ensuring a framework is in place. An assessment of risk maturity enables Council to assess the performance of the Risk Management Framework and to determine whether it is meeting expectations. An assessment provides a roadmap for improvement through identifying opportunities to improve and mature the risk culture.

Council will carry out a self-assessment of risk maturity is based on the VMIA maturity model annually.

TRAINING AND EDUCATION

Risk management training and awareness is recognised as an important requirement for all employees. Training will be designed to increase the knowledge and awareness of employees in a number of risk management topics, which include general risk management, public liability, assessment of risks, fraud and corruption, work, health and safety, business planning and community safety.

In addition to formal training, internal and external specialist advice is available and includes help with identifying and assessing opportunities and risk exposures and the implementation of the principles around developing, implementing and monitoring sustainable control measures.

REPORTING AND ESCALATION

The escalation and reporting process has been established to enable the organisation to:

- Have an understanding of Council's risk exposures as a whole.
- Identify risks that require extensive management attention.
- Provide risk information to the various stakeholders.
- Provide the necessary information for managers at all levels to make risk informed decisions.

Risk Escalation

Risk escalation criteria is the standard upon which risks must be notified in accordance with the materiality of the risk, as ranked in accordance with the risk rating table. It gives the people deemed accountable for the risk every opportunity to address the risk in a timely manner and reduce the likelihood of the risk becoming an event.

Risk Level	Action
Extreme	Must complete control evaluation. Executive Management review required.
High	Must complete control evaluation. General Manager review required and control issues and status reported to EMT.
Medium	Control evaluation where appropriate. Department Manager responsible for controls and reports control issues to General Manager.
Low	Examination of controls is not specifically required. Monitored by Business Unit.

Strategic Risks

Two strategic risks will be considered by the Executive Management Team on a monthly basis and reported to the Audit and Risk Committee biannually. The objectives of this approach are to:

- Ensure that EMT has regular discussion about risk management, and strategic risks in particular, with frequency that embeds risk management in to day to day operations.
- Ensure the Audit and Risk Committee sees regular commitment to risk management and can ask questions as needed.

Operational Risks

Risks with a residual risk rating of High or above, will be escalated to the General Manager monthly, and the serious risks are presented to the Executive Management Team on a quarterly basis where further mitigations and treatment plans are discussed. Operational Risks will be presented to the Audit and Risk Committee on an annual basis.

ACCOUNTABILITIES AND RESPONSIBILITIES

Audit and Risk Committee	• Oversee the risk management activities and review mechanisms in place to comply with the Risk Management Framework: process, resources and effective engagement. • Consider the adequacy of actions taken to ensure that the risks have been dealt with in a timely manner to mitigate exposures to the Council. • Review Council's high cost project risks to ensure adequacy of mitigation strategies are in place.
Council	• Responsible for the adoption of the Risk Management Framework. • Responsible for setting the risk appetite for Council. • Receives and notes reports from the Audit and Risk Committee on the progress of the risk implementation plan and reported risks.
Executive Management Team (EMT)	• Integrate risk management into division/branch activities to drive a strong culture of risk awareness and practice – this involves continually and systematically identifying, analysing, evaluating and treating risks that may impact on objectives. • Responsible for embedding risk management into decision-making and ensuring that risks are managed in accordance with the Risk Management Framework. • Accountable for approval, ownership and management of strategic risks. • Provide executive leadership in the management of strategic, operational and project risks and generally champion risk management within Council.
Managers	• Ensure all the requirements of Council's Risk Management Framework are implemented effectively across their areas of responsibility. • Championing risk management within their department and appropriate risk management practice by employees, volunteers, contractors, and service providers. • Accountable for risk assessments and completion of risk actions in their respective areas of responsibility. • Responsible for ensuring controls in place are working effectively.
Manager Governance	• Responsible for maturing Council's risk management culture through coaching, training and implementing the Risk Management Framework across the organisation. • Ensure that Council's risk management culture is continuously evolving as Council matures. • Provide strategic advice on risk management, resilience and guidance to the CEO, EMT and the Audit and Risk Committee. • Prepare various risk management reports to the Audit and Risk Committee and EMT in accordance with the Risk Management Framework and Audit and Risk Committee Workplan. • Liaise with the Internal Auditor and other stakeholders as required. • Measure risk management maturity and report on the implementation of actions to achieve target maturity.
Risk and Insurance Officer	• Responsible for continuously improving the Risk Management Framework. • Develop, maintain and quality assure enterprise risk registers and monitor implementation of controls and agreed treatment actions. • Assist with the preparation of various risk management reports to the Audit and Risk Committee and EMT in accordance with the Risk Management Framework and Audit and Risk Committee Workplan. • Provide risk management training, advice and support and conduct risk assessments as agreed with EMT or Senior Management.
All Employees	• Responsible for applying risk management practices in their area of work and ensuring that management are aware of the risks associated with Council's operations including recommendation of suitable plans to manage risk. • Seek guidance and support from Risk and Insurance Officer.

PART 4 – REFERENCE AND RELATED DOCUMENTS

AS/NZ ISO 31000:2009 Risk Management Principles and Guidelines

Audit and Risk Committee Charter

Colac Otway Shire Risk Management Procedure

Councillor Code of Conduct

Employee Code of Conduct

Fraud and Corruption Framework

Local Government Act 2020

Occupational Health and Safety Act 2004

Occupational Health and Safety Regulations 2017

Victorian Managed Insurance Authority

Other influencing legislation may include:

- *Equal Opportunity Act 2010*
- *Planning and Environment Act 1987*
- *Public Health and Wellbeing Act 2008*
- *Child Wellbeing and Safety Act 2005*
- *Protected Disclosure Act 2012*
- *Charter of Human Rights and Responsibilities Act 2006*
- *Ombudsman Act 1973*
- *Privacy and Data Protection Act 2014*
- *Road Management Act 2004*
- *Building Act 1983*
- *Wrongs Act 1958*
- *Emergency Management Act 2013*
- *Independent Broad-based Anti-Corruption Commission Act 2011.*

APPENDIX 1 – KEY TERMS AND DEFINITIONS

Communication and consultation	Continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk.
Consequences	Outcome of an event affecting the objectives. • *A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.*
Control	Measure that maintains and or modifies risk. • *Controls are not limited to, any process, policy, device, practice or other conditions and or actions which maintain and or modify risk.* • *Controls may not always exert the intended or assumed modifying effect.*
Establishing the context	Defining the external and internal parameters to be considered when managing risk and setting the scope and risk criteria for the risk management policy.
Event	Occurrence or change of a set of circumstances. • *An event can have one or more occurrences and can have several causes and several consequences.*
External context	External environment in which the organisation seeks to achieve its objectives.
Internal context	Internal environment in which the organisation seeks to achieve its objectives.
Level of risk	Magnitude of a risk or combination of risks expressed in terms of the combination of consequences and their likelihood.
Likelihood	Chance of something happening.
Monitoring	Continual checking; supervising, critically observing or determining the status to identify change from the performance level required or expected.
Residual risk	Risk remaining after risk treatment.
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject to achieve established objectives.
Risk	Effect of uncertainty on objectives. • *An effect is a deviation from the expected. It can be positive, negative, or both and can address, create or result in opportunities or threats.*
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk attitude	Organisation's approach to assessing and eventually pursuing, retaining, taking or turning away from risk.
Risk criteria	Terms of reference against which the significance of a risk is evaluated.

Risk evaluation	Process of comparing the results of risk analysis with the risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
Risk identification	Process of finding, recognising and describing risks.
Risk management	Coordinated activities to direct and control an organisation in relation to risk.
Risk management plan	Scheme within the risk management framework specifying the approach, components and resources to be applied to the management of risk.
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk owner	Person or entity with the accountability and authority to manage a risk.
Risk profile	Description of any set of risks.
Risk source	Element which, either alone or in combination, has the potential to give rise to risk.
Risk treatment	Process to modify a risk.
Stakeholder	Person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity. • *The term interested party can be used as an alternative to stakeholder.*
Reference: AS/NZS ISO 31000:2018 Risk Management–Principles and Guidelines	

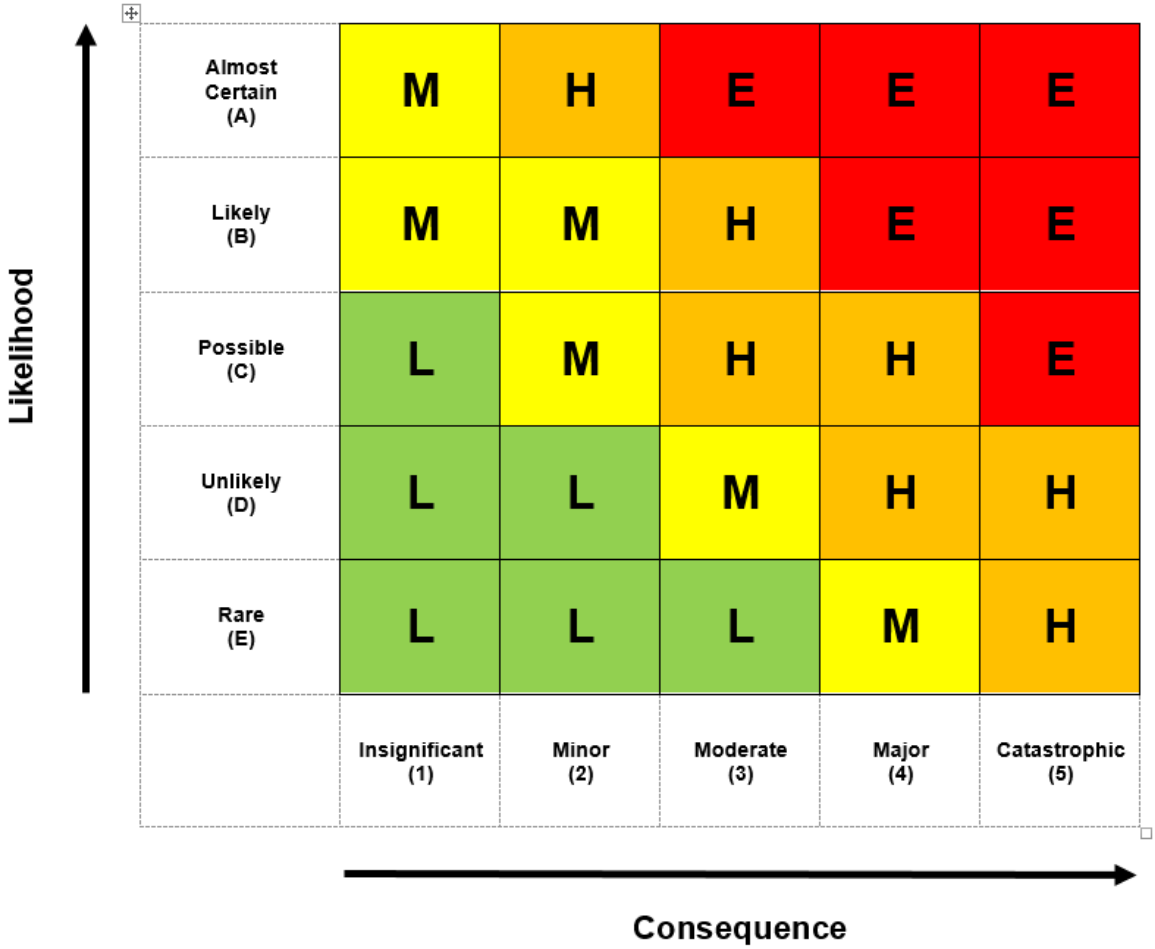
APPENDIX 2 – CORPORATE RISK ASSESSMENT MATRIX

	Category Description	Appetite Statement	CONSEQUENCE				
			Insignificant	Minor	Moderate	Major	Catastrophic
Safety	*Risks relating to managing the physical and general work environment and Council controlled spaces and their impact on health and safety of staff, contractors, volunteers or members of the public.*	*Council has no appetite for work practices, actions or inactions that compromise the wellbeing and safety of people including staff, contractors, volunteers and community.*	Near miss (no injury) OR Minor medical attention without restriction to work (eg Band-Aid or Panadol)	(Physical / mental) Lost Time Injury (LTI) < 30 days OR Injury to staff or public requiring medical treatment or intervention for up to 8 weeks	(Physical / mental) Lost Time Injury (LTI) 30 days to 6 months OR Injury to staff or public requiring medical treatment or intervention for up to 12 months	Permanent disabling injuries or illness where unable to return to the workforce (including serious psychological /mental injury) OR Prosecution for negligence under the Workplace Health and Safety legislation	Loss of life as a result of Council operations
Financial	*Risks associated with the financial management of Council and its ability to fund Council services now and into the future (including risks related to revenue, expenditure, budget management, investments and debt management and accuracy of financial information).*	*Council has a small to medium appetite for variation in financial performance as long as long-term financial sustainability is not threatened.*	Negative financial impact of up to $50,000 etc	Negative financial impact of >$50,000 to $200,000	Negative financial impact of >$200,000 to $1,000,000	Negative financial impact of >$1,000,000 to $5,000,000	Negative financial impact of >$5,000,000
Cyber Security	*Risks relating to the security of the network, applications and information security and disaster recovery.*	*Council has a no appetite for external and internal threats, misuse, modification and unintended damage to the security of its ICT systems/environment.*	A security event without system loss OR A security event without data loss	A security event that results in system loss for <1 day OR A data breach resulting in non-personal information disclosed	A security event that results in system loss for 1 day to 2 weeks OR A data breach resulting in personal information disclosed without further consequence	A security event that results in system loss for >2 weeks OR A data breach resulting in personal information disclosed, leading to identity theft	A security event that results in permanent system loss OR A data breach resulting in personal information of vulnerable people disclosed, leading to harm
Reputation	*Risks relating to negative stakeholder opinion or negative publicity regarding business practices, Council decisions or behaviour of officers and Councillors.*	*Council understands that negative publicity may occur where there is competing priorities and interests in the community. Council has a medium to large appetite for impacts on Council's reputation.*	Community satisfaction with decision making reduced by up to 5% compared to prior year OR General service complaint by one customer OR Less than five repeated negative stories in the local media about the issue	Community satisfaction with decision making reduced by 5-10% compared to prior year OR Complaint by a community group which is escalated in the public arena OR Five to 10 repeated negative stories in the local media about the issue	Community satisfaction with decision making reduced by 10-20% compared to prior year OR Complaints by up to 10 community groups on a single issue that necessitates a public response from Council OR Up to 20 repeated negative stories in regional media about the issue	Community satisfaction with decision making reduced by 20-30% compared to prior year OR Complaints from community groups across the municipality that that escalate to regional or State media OR Repeated negative stories across multiple channels that consumes >50% of executive time for >6 weeks	Community satisfaction with decision making reduced by >30% compared to prior year OR Be named in Parliament by and Integrity of reporting agencies OR Negative media commentary results in workforce resignations >10%
Asset Management	*Risks arising from the potential deterioration, damage or destruction of Council assets and road infrastructure (including both financial costs of repair and/or replacement and the impact that loss of access to the asset has on service delivery).*	*Council has no appetite to compromise on standards that impact on public safety.* *Council has a small to medium appetite and will accept some level of risk over non-core or non-essential assets and infrastructure.*	Localised damage to a single general asset which can be remedied within 6 months OR Widespread damage to a number of general assets that can be remedied within 2 months	Localised damage to a single general asset which can be remedied within 2 years OR Widespread damage to a number of general assets that can be remedied within 12 months	Localised damage to a single critical asset which can be remedied within 3 years OR Widespread damage to a number of general assets that can be remedied within 3 years	Localised damage to a single critical asset which can be remedied within 5 years OR Widespread damage to a number of general assets that can be remedied within 5 years	Widespread damage to a number of critical assets which takes >5 years to remedy OR Total or permanent destruction to one or more critical assets
Environmental Impact	*Risks associated with Council's operations that have potential or actual negative environmental, ecological or cultural heritage impacts, regardless of whether these are reversible or irreversible in nature.*	*Council has a small appetite for risks that cause significant and irreparable damage to the environment and seeks to preserve and enhance it for future generations.*	A single occurrence that causes temporary environmental harm that is not measurable (below detection limits) OR No change in Greenhouse emissions OR Verbal warning received from EPA	A single occurrence that causes temporary environmental harm OR Increase in Greenhouse emissions of >2% OR Written warning received from EPA	Single or repeated occurrences which causes environmental harm which is able to be remediated in <2 years. OR Increase in Greenhouse emissions of >10% OR Remedial notice received from EPA	Single or repeated occurrences which causes environmental harm which is able to be remediated in >2 years and <5 years OR Increase in Greenhouse emissions of >20% OR Infringement notice received from EPA	Single or repeated occurrences that cause ongoing environmental harm that cannot be repaired OR Increase in Greenhouse emissions of >30% OR Court proceedings initiated by EPA

	Category Description	Appetite Statement	CONSEQUENCE				
			Insignificant	Minor	Moderate	Major	Catastrophic
Governance	*Risks relating to regulatory obligations and expectations and good governance framework and principles.*	*Council has small appetite for breaches of legal obligations, good governance principles, policies or contractual agreements that result in fines, penalties or reputational damage.* *Council has zero tolerance for illegal activities including fraud and corruption.*	Non-compliance requires reporting to Audit and Risk Committee OR Councillor or employee conduct matter requiring apology, discussion or training	Minor statutory breach that results in a non-material fine (ie infringement notice) OR Councillor or employee conduct matter requiring internal dispute resolution	Statutory breach that results in a material fine OR Repeated Councillor or employee conduct matters requiring external arbitration or investigation	Statutory breach that results in a significant fine OR Municipal Monitor imposed by Minister	Statutory breach that may result in imprisonment OR Council is sacked and Administrators appointed

Likelihood	Rare (E)	Unlikely (D)	Possible (C)	Likely (B)	Almost Certain (A)
Probability	The event may only occur in exceptional circumstances (0-5% chance)	The event could occur at some time (5-10% chance)	The event should occur at some time (10-30% chance)	The event will probably occur in most circumstances (30-90% chance)	The event is expected to occur in most circumstances (>90% chance)
Frequency	Less than once in 15 years	Once in 10 years	Once in 3 years	Once per year	More than once per year

APPENDIX 3 – RISK RATING MATRIX AND RISK ESCALATION MATRIX



Risk Level	Action
Extreme	Must complete control evaluation. Executive Management review required.
High	Must complete control evaluation. General Manager review required and control issues and status reported to EMT.
Medium	Control evaluation where appropriate. Department Manager responsible for controls and reports control issues to General Manager.
Low	Examination of controls is not specifically required. Monitored by Business Unit.