ACT Government
Transport Canberra and City Services

Framework

Risk Management Framework and Plan

Document ID	Title	
REVISION 2.0	**DOCUMENT OWNER** Executive Branch Manager, Governance and Ministerial Services	**DATE PREPARED** 25/03/2021
TYPE Framework	**APPROVED BY** A/g Director-General	**REVIEW DATE** 25/03/2023
DATE APPROVED **14/04/2021**		

Jim Corrigan
A/g Director-General

Table of Contents

1.0 Risk Management Policy Statement

Transport Canberra and City Services Directorate (TCCS) strives to achieve a strong risk management mindset in our staff, where risk management is not only discussed regularly but integrated into our daily activities. This Framework recognises that risk is inherent in all TCCS's functions and the elimination of all risk is not always practical or appropriate.

The Directorate's risk management approach aims to ensure that:

- risk management aligns with organisational values, behaviours, and objectives
- risk and accountability for risk is understood by everyone
- risks are reviewed regularly, are clear, communicated and documented
- risk informs TCCS's business plans, strategic objectives, and decision-making
- risks and opportunities are identified and used to improve performance
- significant risks are escalated and managed at the appropriate level; and
- a strong and open risk culture is cultivated across TCCS.

Risk management in TCCS is based on the AS ISO 31000:2018 Risk Management Guidelines and the ACT Government Risk Management Policy 2019. The approach to risk management in TCCS supports the ACT Government's commitment to 'managing risk to meet its fiscal, social, and environmental responsibilities'.

All executives and their business units are to demonstrate their commitment to robust risk management and assessment by adopting and implementing the TCCS Risk Management Framework.
TCCS' planning processes, including strategic and business planning, together with organisational policy development and project management will incorporate risk management processes. Risks that are identified, along with their treatment strategies, are to be incorporated into the relevant business planning and/or project management processes.

All staff are responsible for managing risks affecting organisational objectives, program, and project delivery, as well as all other day-to-day aspects of their area of work. Risks should be managed in ways that achieve the best outcomes for the organisation and its stakeholders. Staff are to be provided with information and training on risk management, as appropriate, and will be provided with opportunities to contribute to risk identification, assessment, and management processes. Where possible, opportunities to foster the development of a risk mindset should be encouraged.

Risk management in TCCS is overseen by the Executive Board with recommendations provided to the Audit Committee and the Director-General. This strategic and systematic approach to risk management, aligned with corporate and project objectives, will encourage sound judgements and decision-making and cost-effective use of resources. In addition, this approach will maximise potential opportunities whilst minimising possible adverse consequences.

I look forward to your individual commitment and support in proactively applying the TCCS Risk Management Framework and encourage you to read and implement this Framework in full.

Jim Corrigan
A/g Director-General
Transport Canberra and City Services

2.0 Introduction

2.1 Purpose

The TCCS Risk Management Framework (the Framework) outlines the coordinated and systematic processes that assists TCCS to understand and manage risk. The Framework provides the foundation and organisational arrangement for how risk is managed across the Directorate. The purpose of this Framework is to integrate the process for managing risk into the Directorate's overall governance, strategy and planning, management, reporting processes, policies, values, and culture.

To ensure all known risks impacting TCCS' key deliverables are assessed in a common and systematic way, TCCS maintains a cloud-based Enterprise Risk Management system (Riskware) for recording, monitoring, and reviewing risk. Effective risk management is essential for the development and delivery of quality services across the ACT Government and to the ACT community. It helps in determining an appropriate control environment and strategies to address the risk, ensuring efficient and effective utilisation of Directorate resources.

The Executive Board is committed to the implementation and maintenance of the approach defined in this Framework. Implementation of the Framework contributes to strengthening management practices, decision making and resource allocation, while at the same time protecting the public interest and maintaining trust and confidence.

2.2 Objectives

The key objectives of this Framework are to provide a basis for:

- consistent, confident, and accountable planning and decision-making;
- reliable operations and business activities providing certainty in expected outcomes;
- identifying and taking opportunities to improve performance as well as acting to avoid or reduce the chances of something going wrong;
- anticipating future occurrences and recognising external factors that may impact the organisation;
- excellence in management and encouraging innovation (including by responsible risk taking);
- forward thinking and active approaches to management;
- effective allocation and use of resources;
- sound incident management and reduction in the cost of risk, including insurance and workers' compensation premiums;
- sound stakeholder confidence and trust;
- a clear understanding by all staff of their roles, responsibilities, and authorities for managing risk;
- compliance with relevant legislation and good corporate governance;
- the development of a more risk-aware organisational culture through enhanced communication, skills development and reporting of risk; and
- an appropriate balance between the cost of managing risk and the anticipated benefits.

2.3 Scope

TCCS' Risk Management Framework is consistent with the ACT Insurance Authority Risk Management Policy 2018 and the AS ISO 31000:2018 Risk Management – Principles and Guidelines standard.
This document provides:

- a risk management policy statement clearly stating the Directorate's commitment to risk management;
- an outline of the principles of risk management which are to be applied;

- a Risk Management Plan;
- an overview of the roles and responsibilities for managing risk including risk governance arrangements; and
- details of internal and external communication and reporting mechanisms.

2.4 Application

Application of the Framework is not limited to simply strategic or corporate risks. The process should be applied across all aspects and levels of the Directorate's business and operations.

2.5 Whole of Government Practices

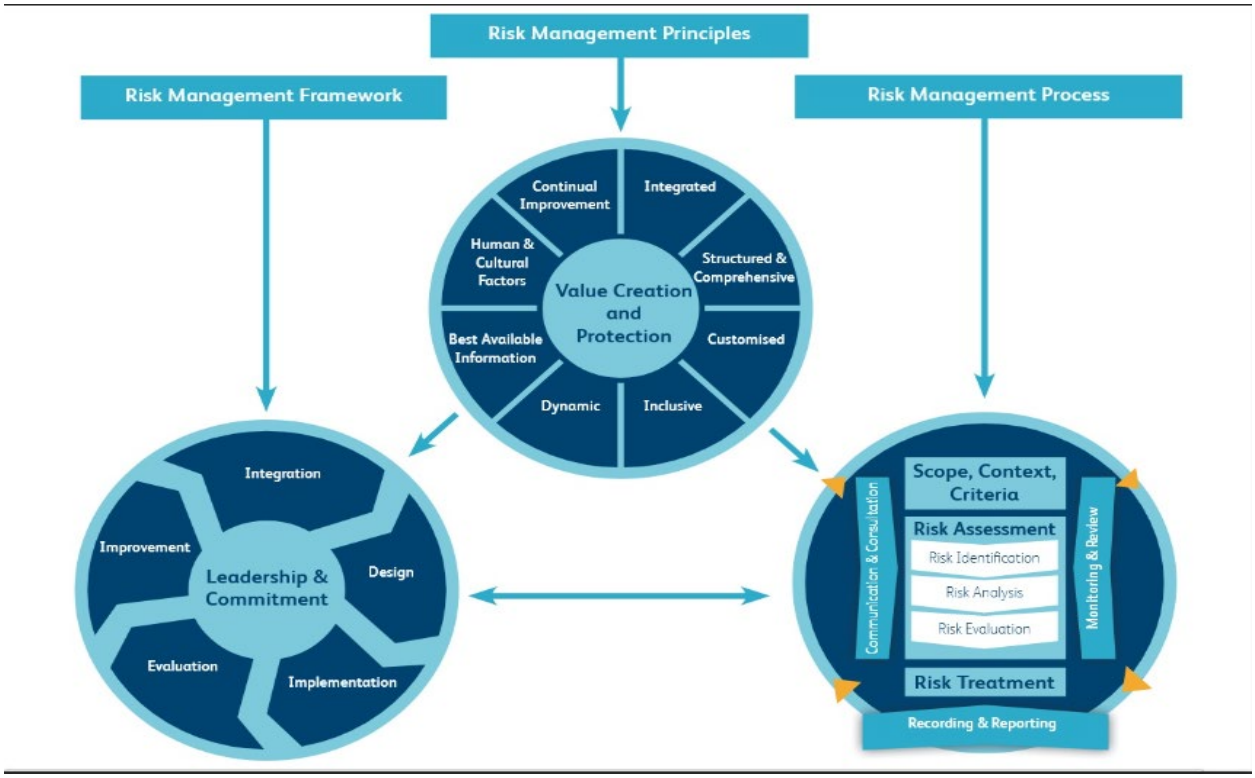
The ACT Government is committed to robust risk management practices, recognising that risk management is an integral part of good management.

The ACT Insurance Authority (ACTIA) is a statutory authority responsible for promoting good risk management practices and advising on the management of Territory risks. ACTIA promotes the adoption of good risk management practices throughout all ACT Government Directorates and organisations. This Framework is consistent with the requirements of the ACT Government Risk Management Framework 2018.

The TCCS Risk Matrix, Enterprise Risk Management System, tools, and templates are based on those developed by ACTIA. These resources have been developed to be consistent with the AS ISO 31000:2018 standard. AS ISO 31000:2018 is separated into three core areas:

- principles;
- framework; and
- process (refer to *TCCS Risk Management Plan* for further details).

The following diagram shows the relationship between the principles of risk management, the Risk Management Framework, and the process for managing risk as set out in the AS ISO 31000:2018 Risk Management Standard.



2.6 Risk definition

The International Standard on Risk Management AS ISO 31000:2018 defines risk as 'the effect of uncertainty on objectives. This definition highlights risk as an uncertainty of outcome. This uncertainty can relate to either a threat or an opportunity and risk management can relate to how we ensure threats do not result in negative consequences and how we ensure opportunities are realised.

2.7 Why we manage risk

AS ISO 31000 defines risk management as 'coordinated activities to direct and control an organisation with regard to risk'. It is the systematic and ongoing process of risk identification, assessment, treatment, and monitoring. It can be applied at any level of TCCS, more notably at the strategic, operational and at project levels. It is not solely about limiting risk but fully appreciating and recognising the risks we have and balancing risk and reward in an informed and decisive manner.

The overarching objective of risk management is to ensure that risk identification, assessment and management occurs continuously in accordance with changes in the internal and external environment and that TCCS has processes in place to enable it to provide assurance to the Director-General, Audit Committee, Executive, and Ministers that risk management processes are effective in controlling and addressing risk.

2.8 Objectives and benefits

The primary objective of sound risk management practice is to support the achievement of the TCCS's strategic and operational objectives, whilst safeguarding our resources, people, assets, finances, knowledge, and reputation.

Adopting a structured and transparent approach to risk management processes within TCCS will enable stakeholders to make informed decisions and ensure that appropriate action is taken to minimise the effect of uncertainty in achieving core business objectives.

2.9 Risk management culture and leadership

The Director-General and the Executive Board provide governance leadership, determine the strategic direction and risk appetite, promote the culture and set the 'tone from the top' to ensure the best outcomes for TCCS, our stakeholders and the community. This is done through:

- defining and communicating what types of risks they will accept and how much risk they will tolerate
- encouraging open and frank communication and reporting of risk, thus ensuring a consistent approach to risk management
- understanding risk principles and coaching the staff to follow them
- setting and modelling expected risk management behaviour
- understanding that human behaviour and culture influence all aspects of risk management, and ensuring TCCS values and behaviours support effective risk management and a no blame culture
- integrating risk management into strategic planning and decision-making; and
- invest appropriate time and resources into training and awareness for all staff, but in particular for managers, nominated risk and control owners, staff with specified risk and emergency management roles, and staff working in high-risk areas of the directorate.

3.0 Risk Management Principles

The principles of risk management when embedded within our Directorate enable the Executive and staff to create and protect organisational value. Risk management contributes to the achievement of our objectives and improves performance in areas such as corporate governance, program and project management, security, legal and regulatory compliance, environmental protection, and health and safety. AS ISO 31000:2018 is based on **8** best practice principles.

1. **Integrated: Risk management is an integral part of all organisational processes** - risk management is not a stand-alone activity performed in isolation. Rather, it is an integral part of our governance and accountability arrangements, performance management, planning, and reporting processes.

2. **Structured and Comprehensive: risk management is systematic, structured, and timely** - risk management contributes to efficiency and to consistent, comparable, and reliable results.

3. **Customised**: **Risk management is tailored and customised** to ensure that all risk management components (Framework and Processes) are proportionate to and align with the internal and external environment within which we operate and is managed in the context of our Directorates objectives.

4. **Inclusive: Risk management is inclusive** - risk management requires appropriate and timely involvement of stakeholders to ensure that it stays relevant and up to date. Involving stakeholders enables their knowledge, views, and perceptions to be considered.

5. **Dynamic: Risk management is dynamic, iterative, and responsive to change -** risk management anticipates, detects, acknowledges, and responds swiftly to both internal and external events, changes in the environmental context and knowledge, results of monitoring and reviewing activities, new risks that emerge and others that change or disappear.

6. **Best Available Information: Risk management is based on the best available information:** risk management should draw on diverse sources of information, as well as consider future expectations. Historical data, expert judgment and stakeholder feedback all contribute to make evidence-based decisions. As decision-makers, we should be cognisant of the limitations of data, modelling and divergence among experts.

7. **Human and Cultural - Risk management considers human and cultural factors -** risk management recognises that human behaviour and culture influence all aspects of risk management. The capabilities, perceptions and aims of people (internal and external) can aid or hinder the achievement of objectives.

8. **Continual Improvement - Risk management contributes to the continual improvement of the organisation** – risk management facilitates continuous improvement of our operations by developing and implementing strategies to improve risk management maturity. Risk management practices are continually improved through the application of learning and experience.

4.0 Risk Management Process

4.1 TCCS management of risk

In accordance with the ACT Government Risk Management Policy 2019, TCCS has implemented a minimum six-monthly review cycle of divisional risk registers, unless triggered by a large change in the operational or strategic environment. These reviews should be undertaken to support the TCCS strategic and business planning cycles, and subsequent organisational deliverables. To help ensure that new and emerging risks are not overlooked, a rigorous and systematic approach to identifying and adequately managing risks at strategic and operational level is essential.

TCCS performs a diverse range of activities, at both the strategic and operational levels, and recognises that not all known risks can be easily captured, reviewed, and reported on within specified timeframes. It is therefore important that each business area within TCCS maintains a risk profile that is tailored to support effective risk governance and decision-making processes. In order to simplify this process, TCCS has implemented an Enterprise Risk Management System that provides the flexibility and capability to accept risk, archive risk, and share known risks between business areas.

Risk management is an ever-present responsibility. All staff are required to be conversant with risk management and be able to utilise and demonstrate application of risk management principles within their areas of control. Staff familiar with the work undertaken in specific areas are well placed to identify risks in their own areas and recommend suitable strategies for controlling the impact of those risks.

4.2 Process overview

TCCS's Risk Management process complies with AS ISO 31000:2018. Under this approach, there are six stages to the risk management process.

1. Communicate and Consult - with internal and external stakeholders.
2. Establish Context - the boundaries, scope, and criteria.
3. Risk Assessment - identify, analyse, and evaluate risks.
4. Treat Risks - implement and assess controls to address risk.
5. Monitoring and Review - risk reviews and audit.
6. Recording and Reporting - ensuring the appropriate levels of management are informed.

4.3 Managing risk within a diverse portfolio

The identification and management of risk is best undertaken by those closest to the risk. That is, the business area responsible for the effective delivery of government and directorate objectives and services, including those with responsibility over the operational risk control environment. Risk ownership will generally sit with the executive branch managers or officer with the appropriate delegations in respect of decision-making authority, and allocation of funding to mitigate the risk.

The ACT Insurance Authority (ACTIA) has overarching policy responsibility for risk management in the ACT Public Service. TCCS has adopted ACTIA's guidance and refined the following list of potential categories of risk for use in the development of risk registers and plans. In defining strategic, operational and project risk, consideration should be given, but not limited to the following risk categories when developing and reviewing risk management plans:

- Workplace Health and Safety (WHS)
- assets, business processes and systems
- compliance and regulation
- products, services, and technology (includes information, records management, and data security)
- cultural, heritage, environmental and climate
- financial, people and general business management activities; and
- reputation and image.

The directorates risk matrix at Attachment A and Enterprise Risk Management System further support and define the primary risk categories and risk consequence descriptors.

The model below outlines how managing risk at strategic and operational levels of the organisation aims to support the delivery of our strategic objectives and the delivery of customer centric services.

4.4 New and emerging risk identification and risk escalation

Risk escalation elevates shared ownership and accountability for an extreme or high risk to the most appropriate risk owner, which is usually a senior executive. Risks with strategic implications rated as High or Extreme after controls have been considered and applied, need to be reported through normal

organisational reporting lines. This aims to ensure that High or Extreme risks are escalated to an appropriate level of authority and to ensure a shared understanding of the risk. The table below indicates priority for attention in respect of new and emerging risks.

Perceived Risk level	Notification and escalation of a new or emerging risk	Risk assessment and risk treatment action plan	Reported to/approving authority	Additional reporting considerations
Extreme	A soon as possible, or within 24 hours	1 month or sooner	DG, DDG/s and COO	Minister Chief Audit Executive Chair Audit Committee Other impacted Boards, Committees or working groups
High	As soon as possible or within 2-7 days	2 months or sooner	DDG/COO/Executive Group Manager	Minister Chief Audit Executive Chair Audit Committee Other impacted Boards, Committees or working groups
Medium	Within 1 month	3 months or sooner	Executive Branch Manager/Business Unit Head	Impacted Boards, Committees or working groups
Low	Within 3 months or in course of normal business	3-6 months or through 6 monthly review cycle	Executive Branch Manager/Team Leader	Impacted Boards, Committees or working groups

Every care should be taken to act as soon as possible to implement risk control measures wherever possible or to take action to address issues arising. Extreme and High risks, especially where the risk relates to people and community safety or personal injury, require TCCS to act immediately and take steps to put controls in place to reduce the likelihood of consequence of the risk event.

The suggested timing of treatment is a guide and wherever possible immediate action should be taken to control the risk as soon as possible, noting that if a risk is identified which is critical to the health and safety of staff then it needs to be dealt with immediately.

4.5 Shared risks

Shared risks are those that may extend beyond TCCS and involve other entities, or cross multiple parts of TCCS. These risks still have a potential to impact TCCS and will be recorded within divisional level and project level risk registers as required. They are to be managed in accordance with the TCCS Risk Management Framework and associated risk governance mechanisms.

Shared risks may include, but are not limited to, inter-directorate and cross-directorate activities and programs, third party contract agreements, partnerships, and procurements. Insurance arrangements will be implemented and executed to cover insurable risk. Examples of shared risk include the potential impact of the light rail transport network and future light rail stages have on directorate planning and operational activities. Impacted areas may include, Roads ACT, City Presentation, Development Planning, Bus Operations, Infrastructure Delivery, Legal, Governance and ACT NoWaste.

To effectively manage these impacts TCCS Light Rail Operations have established a Risk and Change Management Committee (RCMC) to share and discuss risk with a broad range of stakeholders and seek feedback on shared risk, including defining controls and treatment for action. Key TCCS executives have roles and responsibilities within the RCMC where risk is reported and discussed.

4.6 TCCS Risk Management Plan

The TCCS Risk Management Plan, at Appendix B supports the achievement of strategic and operational goals by providing a structure for all levels of management to enable, support and promote:

- awareness and understanding of the real and significant business risks and their impact;
- demonstration of due diligence in decision-making
- exercise of appropriate duty of care
- innovation through the taking of calculated risks in pursuit of business opportunity and excellence
- provision of assurance that business risks are properly managed, commensurate with their level of threat or exposure; and
- key risk management performance indicators to enable compliance and continuous improvement of the framework, core TCCS values and organisational culture.

4.7 Business level risk assessments

Executive Branch Managers (EBM) are ultimately responsible for ensuring risks within their division are captured within their risk profile/s and are maintained within the terms on the Framework. EBMs will be the risk owner for risks within the span of their control. However, EBM's, may nominate a responsible officer to manage the risk control environment, ensure the effectiveness of controls within their span of responsibility, including the implementation of risk treatment and corrective action items. EBMs are also required to communicate new high or emerging risks to their Executive Director, Deputy Director General or Director General as appropriate. The following table outlines the process TCCS follows to manage completed risk assessments.

Process	Description	Responsibility
Management of risk	1. Output from risk assessments to be held in Risk Registers. ▪ TCCS' Enterprise Risk Management system provides a single platform for strategic and operational risk profiles. ▪ WHS hazard specific registers are to be held in registers as defined within the entity's safety management system. ▪ The ACT Insurance Authority (ACTIA) maintains templates for all government entities to utilise as required.	Executive Branch Managers
	2. Risk controls and their perceived effectiveness should align with risk source and causal factors.	Executive Branch Managers, and or nominated action officer
	3. Management responsibility and/or Risk ownership to be identified within risk assessment.	Executive Branch Managers, and or Executive Group Manager
	4. If required, risk treatment actions are to be allocated to nominated task owners and tracked and monitored for completion and measurable (or observable) effectiveness.	Executive Branch Managers
	5. Regular reviews identifying new or emerging risks that might affect the achievement of strategic and business plan objectives and budgets.	Executive Branch Managers, and or Executive Group Manager
Review cycles	6. Reviews of existing business risks will be undertaken at a minimum of 6 monthly including, defining control effectiveness, identifying new risk treatment	Executive Branch Managers, and or Executive Group Manager

	opportunities, and updating the progress with risk treatment action items.	
	7. Program/Project Managers are to conduct reviews of existing risks on a regular basis in accordance with program/project management requirements.	Program/Project Managers, and or Steering Committee/ Board
Reporting	8. Report identified risks and review outcomes to the relevant Executive.	Executive Branch Managers, and or Executive Group Manager
	9. Program/Project Managers will report identified program risks and any identified risk owner to the Program Steering Committee, Program Board or Sponsor Manager/ Executive.	Program/Project Managers, and or Steering Committee/ Board
	10. Risk reporting to both executive board and audit committee will be undertaken on a cyclical basis.	Assistant Director Risk and Business Assurance

4.8 Assessing and measuring risk

Consistent with the whole of government guideline, TCCS will apply the 5x5 risk matrix defined by the ACT Insurance Authority to analyse and evaluate risk consistently across the directorate.

RISK MATRIX		Impact	Insignificant	Minor	Moderate	Major	Catastrophic
Frequency		Matrix	1	2	3	4	5
Likelihood	Almost Certain	5	Medium	High	High	Extreme	Extreme
	Likely	4	Medium	Medium	High	High	Extreme
	Possible	3	Low	Medium	Medium	High	Extreme
	Unlikely	2	Low	Medium	Medium	High	High
	Rare	1	Low	Low	Medium	Medium	High

A detailed risk assessment table, Appendix A, supporting the whole of government guideline has been tailored to meet the needs of our diverse portfolio.

4.9 Risk register development and review cycles

The diagram below refers to the cycle to undertake risk register development and review that aligns with annual business unit planning and mid-year business plan reviews.

1. Risk Register Development and Review

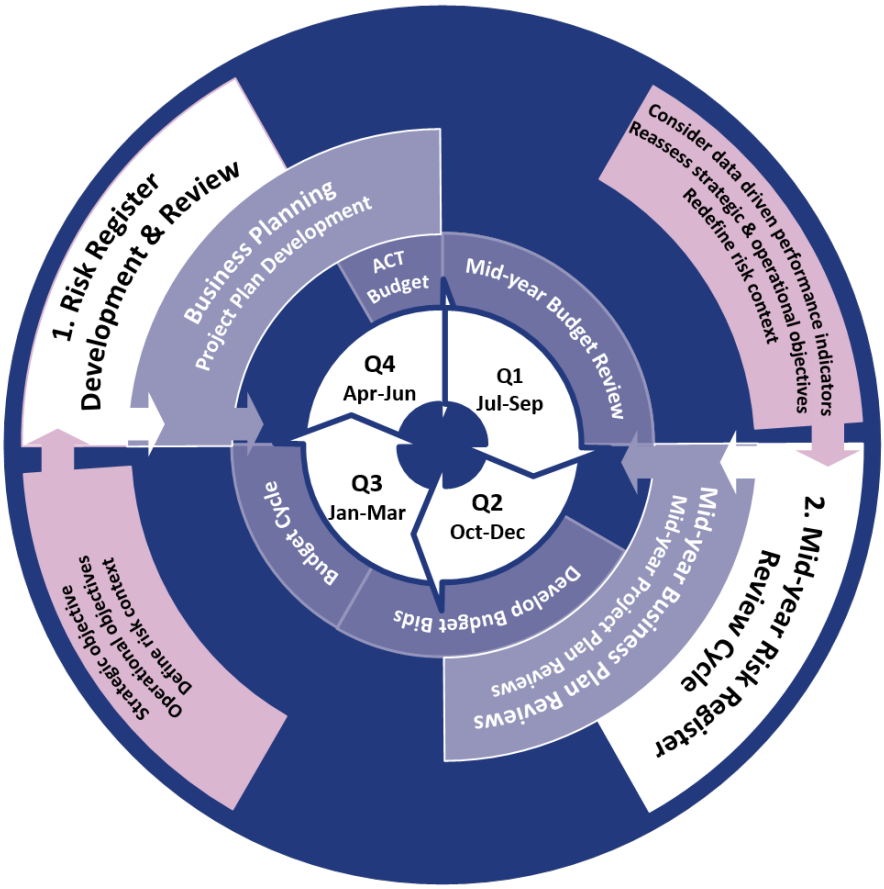
Risk Registers should be developed and/or reviewed considering the current strategic and operational objectives of the business.

Registers should be reviewed as part of annual strategic and business planning cycles.

The adequacy of key controls and their effectiveness should be considered to ensure effective achievement of objectives.

Risk treatment actions should be clearly defined and support the effective allocation of operational budgets or used to inform budget bids.

Regular assessment and review should assist business areas to make well informed decisions.



2. Mid-Year Risk Register Review Cycle

Risk registers should be reviewed considering progress against key objectives and milestones.

The review should align with the mid-year (6 monthly) business planning cycle review.

New risks may need to be defined based on significant changes to the business context.

Control effectiveness should be considered based on business performance (both positive and negative).

Corrective actions may need to be applied to further treat risk and/or inform the budget review process to address longer term treatments.

Emerging risks should be escalated, and treatment actions applied to assist in achievement of strategic and operational objectives.

5.0 Risk Governance

5.1 Risk appetite guideline

TCCS recognises that risk cannot be eliminated at all levels of our diverse organisation, but it can be used as a guide to protect our staff, our community, and our government in achieving our social, economic, and regulatory objectives. The Executive Board has overarching responsibility in setting and refining the directorate's overall risk appetite and tolerance for maintaining high and extreme risks impacting the directorate's strategic objectives. Risk treatment action plans will be developed for all extreme and high risks, where deficiencies in the risk control environment exist. TCCS also recognises that opportunities too can come from risks identified and aim to ensure the early identification and management of new and emerging risks is openly practiced ensuring opportunities can be assessed. All risks will be managed systematically to ensure the risk control environment remains robust, and ongoing tolerance for the level of risk accepted by an appropriate level of authority.

TCCS will use risk management as a tool to minimise exposure to risks relating to the safety, security, and wellbeing of all TCCS employees and customer facing services. TCCS will implement risk management strategies to ensure our services are delivered efficiently, effectively and with respect, integrity, and transparency, reducing exposure to financial, social, environmental, cultural, and regulatory risk.

TCCS will seek to deliver innovative and progressive services, in order to future proof our city, capitalising on opportunities utilising a risk-based approach to aide in decision-making. Known, emerging, and new risks will be managed within the guidelines set out in the ACT Government Risk Management Policy and legislative frameworks set by government.

In applying effective risk management practices TCCS will endeavour to pursue a risk verses reward mindset, to ensure a sensible and measured approach to taking, accepting, and treating risk. Risk management practices will also, support the governments strategic agenda and TCCS' commitment to serving the community.

5.1.1 Strategic risk appetite and tolerance

The TCCS Executive Board have ultimate responsibility for maintaining and monitoring the TCCS strategic risk profile. The strategic risks have been defined to include a risk appetite statement and tolerance levels for consideration of TCCS business areas when assessing and monitoring risk, and performance indicators within their areas of responsibility. The strategic risk profile will be maintained within the enterprise risk management system. A strategic risk appetite and tolerance guideline will be made available to all staff, to ensure visibility and a common understanding of appetite and tolerance understood across TCCS.

5.2 Roles and responsibilities

Risk governance mechanisms embed into TCCS's organisational culture and aim to ensure transparency, accountability and the appropriate level of authority is aligned with the end-to-end management of risk within the Directorate. Roles and accountabilities within TCCS are outlined as follows:

5.2.1 Executive Board

- approve the TCCS Risk Management Framework
- oversee the Directorate's risk profile, including fraud and integrity risks
- endorse the Directorate's strategic risk appetite statement, and establish parameters for strategic risk exposure and tolerance levels

- review of the strategic risk registers for currency every six months, or more frequently as required
- ongoing consultation of intergovernmental risks and treatments where appropriate; and
- review and note risk reports as required.

5.2.2 Executive Leadership Team

- implementation of the TCCS's Risk Management Framework, policy and plans within their respective areas of responsibility
- incorporating risk management principles into all aspects of business operations including business planning activities and day to day operations
- alignment of risk management practices to meet organisational strategic objectives, strategies, and key performance indicators
- ensuring that business plans clearly include discussion on key issues and major risks
- ensuring staff and contractors understand and fulfil their risk management responsibilities
- ensuring that project plans incorporate risk management process that are tailored to align with scope, magnitude, and complexity of the project
- development, ownership, and maintenance of risks indicative of their respective areas of responsibility, including, identifying, analysing, evaluating, and treating risks in a manner proportionate with the level of risk exposure
- ensure the effectiveness of key risk controls within their span of responsibility by:
    - actively participating in the development and execution of internal audit and compliance programs;
    - monitoring business performance, and key performance indicators to make informed decisions about control effectiveness and apply any subsequent corrective actions; and
    - commitment to implement and monitor quality management systems within their business areas
- encourage innovation and taking advantage of emerging risk opportunities to optimise outcomes in a cost-effective manner and consistent with the risk management principles; and
- reporting and providing advice to the Executive Board on risk management matters including escalating risk management issues when appropriate.

5.2.3 Senior Directors and Directors

- promotion of and adherence to the TCCS Risk Management Framework within respective areas of responsibility
- fostering a risk aware culture by creating an environment where managing risks forms the basis of all activities
- encouraging staff to develop risk management skills, and actively participate in risk management processes
- development, ownership, and maintenance of operational risk registers including, identifying, analysing, evaluating, and treating risks that may impact on divisional/team objectives
- regular review of the adequacy of internal controls to ensure the intended level of risk exposure is maintained, fit for purpose, and align with organisational goals and objectives; and
- reporting and providing advice to the executive on risk management matters including escalating risk management issues when appropriate.

5.2.4 Staff and contractors

- understand and adhere to policies and procedures relevant to what they do
- report incidents to their manager or supervisor as they become aware of them; and
- understand the risks in their area.

5.2.5 Program Managers and Project Managers

- develop risk management plans consistent with the TCCS Risk Management Framework, TCCS Project Management Framework, and/or Capital Framework as required
- clearly establish a risk governance structure and define how risks will be managed and reported on throughout the lifecycle of the Program/Project
- development, ownership, and maintenance of program/project risk registers, including, identifying, analysing, evaluating, and treating risks that may impact on program/project deliverables
- regular review of the adequacy of internal controls to ensure the intended level of risk exposure is maintained, fit for purpose, and align with program/project deliverables; and
- compliance with all legislative, regulatory, and organisational policies and procedures.

5.2.6 Audit Committee

- endorse the entities risk management framework
- assess and review implementation of the Directorate's risk management framework
- review currency of the strategic risk register in line with Executive Board review; and
- review and monitor annual assurance program focusing on operations, compliance and fraud and integrity risks.

5.2.7 Internal Audit

- the Chief Audit Executive (CAE), in consultation with the Director-General, recommends an audit and assurance program to the Audit Committee focusing on risks identified in the strategic and operational risk profiles; and
- conducts independent reviews in relation to key risk areas including fraud and integrity risks.

6.0 Three Lines Model

The 'Three Lines of Defence model' provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and responsibilities within TCCS. This model is recommended by the ACT Government Risk Management Policy 2019.

6.1 First line (risk ownership)

Under the first line of defence, operational management has ownership, responsibility, and accountability for directly assessing, controlling, and mitigating risks.

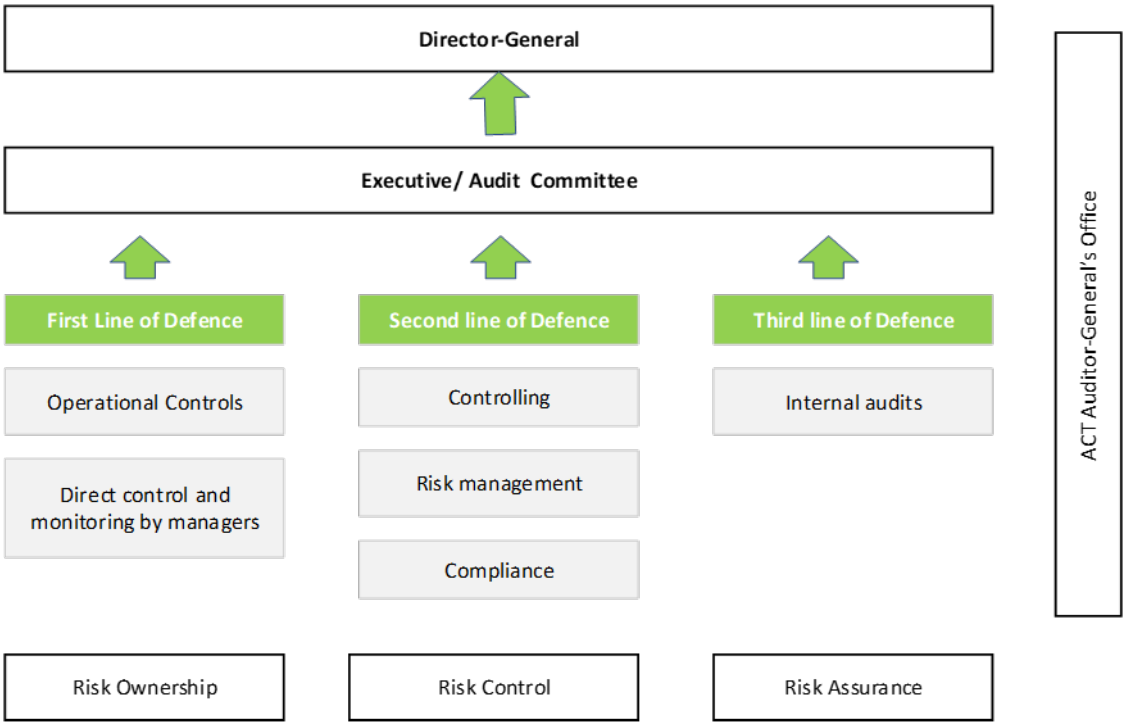
6.2 Second line (risk control)

The second line of defence consists of activities covered by several components of internal governance (compliance, risk management, quality, IT, and other control measures). This line of defence monitors and facilitates the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk related information up and down the organisation.

6.3 Third line (risk assurance)

Internal audit forms the organisation's third line of defence. An independent internal audit function will, through a risk-based approach to its work, provide assurance to the Executive Board and Audit Committee. This assurance will cover how effectively the organisation assesses and manages its risks and will include assurance on the effectiveness of the first and second lines of defence. It encompasses all elements of the TCCS Risk Management Framework. Internal audit should use a risk-based approach in developing and executing the internal audit plan in order to focus on the greatest threats to the organisation.

The use of the three lines of defence to understand the system of internal control and risk management should not be regarded as an automatic guarantee of success. All three lines need to work effectively with each other and with the Audit Committee in order to create the right conditions.



Appendix A: TCCS Risk Matrix

Impact	Insignificant	Minor	Moderate	Major	Catastrophic
1. People (Health & Safety)	Near miss no injuries	Minor injury or requiring First Aid treatment or short-term injury (less than four weeks. and/or minor psychological injury.	Single injury causing hospitalisation or multiple medical treatment cases; and/or psychological injury resulting in GP/Health Professional help.	Serious injury (including loss of limbs) or multiple serious injuries causing hospitalisation and/or permanent disability; and/or psychological injury requiring medium professional support.	Single or multiple Deaths or multiple life-threatening injuries; and/or psychological injury requiring long term professional support.
2. Financial	Less than 1% of **Budget**	1% to 5% of **Budget**	> 5% to 10% of **Budget**	> 10% to 25% of **Budget**	> than 25% of **Budget**
3. Reputation & Image	**Public Confidence:** Minor dissatisfaction across a small proportion of the community and or stakeholder groups. **Media:** Isolated negative local media attention. **Govt Scrutiny:** Internal Review.	**Public Confidence:** Moderate dissatisfaction across a small proportion of the community and or stakeholder groups. **Media:** Negative Local media attention across multiple channels. **Govt Scrutiny:** Scrutiny required by internal committees or internal audit to prevent escalation.	**Public Confidence:** Dissatisfaction across a few demographics groups and or moderate dissatisfaction across multiple stakeholder groups. **Media:** Adverse national or sustained local media attention.(up to one week) **Govt Scrutiny:** Scrutiny required by external committees or ACT Auditor General's Office, or inquest, etc.	**Public Confidence:** Dissatisfaction across a large range of demographics groups. Major dissatisfaction across multiple stakeholder groups. **Media:** Sustained adverse national media attention across multiple media channels. (more than one week) **Govt Scrutiny:** Legislative Assembly scrutiny; Minister/Chief Minister involvement.	**Public Confidence:** Whole community dissatisfaction. Severe dissatisfaction across ALL stakeholder groups. **Media:** Adverse International media attention across multiple media channels. **Govt Scrutiny:** Ministerial/Assembly inquiry or Coronial inquiry.
4. Compliance & Regulation	Non-compliance with policy, contract or standard operating procedures which are not legislated or regulated.	Numerous instances of non-compliance with policy, contract or standard operating procedures which are not legislated or regulated.	Non-compliance with policy, contract or standard operating procedures which require self reporting to the appropriate regulator and immediate rectification.	Restriction of business operations by regulator due to non-compliance with guidelines and / or significant non-compliance with policy , contract or procedures which threaten business delivery.	Operations shut down by regulator for failing to comply with relevant legislation/regulations /or significant non-compliance with could result in failure to provide business objectives and critical service delivery.
5. Service Delivery (Products & Services)	**Business Continuity:** Loss of, or interruption to non-critical infrastructure or essential services up to 3 days. **Strategic Objectives:** Negligible impact on business outcomes. KPI's relating to delivery of strategic objectives not threatened.	**Business Continuity:** Interruption to core services affecting critical infrastructure or public safety or cessation of essential services for up to 3 days. **Strategic Objectives:** Minor impact on business outcomes and/or strategic objectives.	**Business Continuity:** Cessation of essential service ; infrastructure or public safety for up to 3 days and/or disruptions for up to 1 week. **Strategic Objectives:** Moderate impact on business outcomes and/or strategic objectives. One or more key accountability requirements not met.	**Business Continuity:** Cessation of business essential services for up to 3 days and/or continual disruption over subsequent weeks. **Strategic Objectives:** Significant impact on business outcomes and/or strategic objectives. Strategies not consistent with Government's agenda. KPI's show services are degraded.	**Business Continuity:** Total cessation of core services affecting critical infrastructure or public safety Cessation of services essential to business continuity for more than 1 week and/or continual disruption over subsequent months. **Strategic Objectives:** Strategic business processes fail and business objectives not met. Critical system failure/s Business severely affected.
6. Environment & Sustainability	Limited effect to environment, culture or something of low significance. Effects are limited to a small area, with a rapid recovery.	Transient, repairable. Minor effects to cultural or heritage items, environment including disturbance of native vegetation or waterways.	Moderate, short-term harm to cultural or heritage items or environment and/or disturbance of native vegetation or waterways. Mostly repairable.	Significant, medium-term harm. Major impacts to environment, threatened species or habitat, and/or damage to large area of native vegetation or waterways. Permanent damage to structures or items of cultural significance.	Long term environmental harm. Widespread impacts to environment, threatened species, native vegetation or waterways. Irreparable damage to, or loss of highly valued items of cultural and/ or heritage significance
7. ICT Systems & Record Management	Interruption to **electronic records, data and systems** access less than ½ day. **Systems breach** identified, business administration system, no personal or classified information stored.	Interruption to **electronic records, data and systems** access ½ to 1day. **Systems breach** identified, business administration system, some identifiable information stored, non client welfare threatening (data accessed known)	Significant interruption (but not permanent loss) to **data and electronic records access**, lasting 1 - 7 days. **Systems breach** identified, business administration system, some identifiable information stored, non client welfare threatening (data accessed unknown)	Complete, permanent loss of some **electronic records and/or data**, or loss of **systems** access for more than 7 days. **Systems breach** identified, business administration system, identifiable/classified information stored, non client welfare threatening	Complete, permanent loss of all **electronic records, data or system access.** **Systems breach**, Government or business Critical Systems client and or business welfare threatened
8. Integrated Public Transport Network	Unplanned network interruption resulting in cessation of services up to 10 minutes.	Unplanned network interruption resulting in cessation of services for between 10 and 30 minutes.	Unplanned network interruption resulting in cessation of services > 30 mins up to 4 hours.	Unplanned network interruption resulting in cessation of services > 4 hours up to 1 day.	Unplanned network interruption resulting in cessation of services for more than 2 days.
9. Project Delivery	**Schedule Delay:** Delays Less than 2 weeks impacting on achievement of key objectives or milestones. **Quality:** Single minor design and or quality issues – aesthetics.	**Schedule Delay:** Delays 2 - 4 weeks (inclusive) impacting on achievement of key objectives or milestones. **Quality:** Multiple minor design and or quality issues – aesthetics.	**Schedule Delay:** Delays 4 - 8 weeks (inclusive) impacting on achievement of key objectives or milestones. **Quality:** Single moderate design and or quality issue – fit for purpose, customer experience, urban design	**Schedule Delay:** Delays 8 - 12 weeks (inclusive) impacting on achievement of key objectives or milestones. **Quality:** Single major design and or quality issue – safety, design longevity and or performance or multiple moderate quality issues – fit for purpose, customer experience, urban design	**Schedule Delay:** Delays greater than 12 weeks impacting on achievement of key objectives or milestones. **Quality:** Multiple major design and or quality issues – safety, design longevity and or performance

Frequency			Matrix	1	2	3	4	5
Likelihood	Almost Certain	*Almost certainly will occur or Is expected to occur in most circumstances*	5	Medium	High	High	Extreme	Extreme
	Likely	*Will probably occur or Is likely to occur in the current or future environment.*	4	Medium	Medium	High	High	Extreme
	Possible	*Might occur at some time in the future or Will possibly occur in the current or future environment.*	3	Low	Medium	Medium	High	Extreme
	Unlikely	*Could occur but doubtful or is unlikely to occur in the current or future environment.*	2	Low	Medium	Medium	High	High
	Rare	*May occur but only in exceptional circumstances or May occur in rare circumstances only.*	1	Low	Low	Medium	Medium	High

Appendix B: TCCS Risk Management Plan

The TCCS Risk Management Plan provides a detailed guide to support the effective implementation of our Risk Management Framework and outlines our risk management process, including identification, assessment and reporting of risks. The plan aims to minimises our exposure to significant risks and enhance our ability to capitalise on opportunities through minimising risk and improving overall key performance indicators.

Risk Governance	Description	Responsibility	Frequency
Risk Management Framework	A review every two years of the framework allows the organisation to continually improve its processes without deviating too far from the policy and procedures. Endorsement for the framework is sought through Executive Board and Audit Committee and signed off by the Director-General.	Chief Operating Officer/Governance	2 Years
Strategic risk register	The Executive Board will maintain the entity's strategic risk register. In line with the strategic planning process, the Executive Board is responsible and accountable for identifying and managing strategic risks related to our organisational outcomes and impacts.	Director-General/ Executive Board	6 Monthly Q1 – Jul-Sep & Q3 – Jan-Mar
Divisional risk registers	Each TCCS Division must develop and maintain a risk register tailored to meet the strategic and operational objectives of the division. Business units are responsible for identifying, considering, and managing risks associated with their day-to-day operations and the delivery of their products and services. Identification of risks must be done in accordance with the business planning cycle. The relevance of operational risks must be considered in relation to our strategic objectives, and how these objectives may be affected. Operational risks that may impact on or influence strategic objectives should be communicated to the risk and business assurance team. Responsibility for treating these risks will remain with the business unit or relevant area.	Executive Group Managers/Executive Branch Managers	6 Monthly Q4 – Apr-Jun & Q2 – Oct-Dec
Risk assessments	Formal risk assessment workshops are to be undertaken to support the identification of new and emerging risks, proportionate to the activity undertaken, and/or perceived level of risk as defined within the risk management framework. A systematic approach to reviewing strategic and operational risk profiles, is to be integrated as part of the TCCS strategic planning and business planning cycles, to assist and inform decision making processes.	All Business Units	As required
Risk treatment plans	Risk treatment plans exist where a risk has been rated as either extreme or high, or the control effectiveness has been rated as less than effective. These treatment plans are reviewed on a regular basis by the risk, control, and treatment	Risk Owners/ Responsible Officers	6 Monthly Q4 – Apr-Jun & Q2 – Oct-Dec

Monitor and review risk profiles	This allows for lessons learned to be identified and applied to continuously improve risk management maturity, reinforce controls effectiveness, and enhance awareness of risk. This encourages and increases the successful achievement of strategic and business objectives.	Executive Branch Managers	6 Monthly Q4 – Apr-Jun & Q2 – Oct-Dec
Risk management reporting process	All risk registers should be endorsed by the Executive Group Manager. It is the responsibility of the Executive Branch Manager to report and escalate any new or emerging risks, and or significant changes to the risk profile. Risk profile reports are provided to the Audit Committee on a quarterly basis. The risk report identifies the number and severity of risks within each division, and compliance with the risk management framework. All new high and emerging risks are also reported as required. Executive Group Managers are to present at least annually a business briefing to the audit committing, outlining key divisional risks and how they are being managed	Executive Group Managers/ Executive Branch Managers	As required
Communication and consultation	Communication and consultation occur on a regular basis to ensure key stakeholders (both internal and external) are consulted, engaged, and actively involved throughout the risk management process. This promotes a consolidated awareness of the TCCS risk management system and influences behaviour in relation to management of risks.	All Business Units/ Governance	6 monthly
Training and education	ACTIA provide quarterly training opportunities to all ACT Government employees, available through their website. It is recommended that all staff should complete the eLearning module on the TCCS 'My Learning' platform in 'Introduction to Risk in ACT Government' and in respect of Senior Officers, 'Practical application of Risk Management'. Tailored workshops for Business Units can be provided through Governance or ACTIA if requested by the business area or responsible executive.	All staff / Governance	As required
Risk assessment tools and resources	ACTIA Risk Management Implementation Guideline ACTIA Risk Management Office (RMO) tools and resources TCCS Intranet maintains a list of risk management tools and tips to support the effective application of risk management TCCS' enterprise risk management system maintains FAQs and risk management tips through the risk assessment process.	As required	EBM GAMS

Management Activities supporting robust risk management practices

Activity	Description	Frequency	Responsibility
Business Continuity Planning (BCP), business interruption and risk to service delivery	TCCS undertakes business continuity management as a proactive risk treatment to manage disruption-related risks. BCP's are a risk treatment designed to reduce the consequence(s) of a business interruption event. Business continuity management involves the following key steps: • conducting or reviewing a business impact analysis; • development or review of response strategies; • identification or review of resource requirements; • development of, or updating an existing of BCP; and • monitoring, reviewing, and testing on BCPs. Key risks relating to business interruption will be maintained within divisional risk profiles.	Annually	Security and Emergency Management/ Governance
Strategic asset management	Strategic Asset Management Plans (SAMP) underpin the way each business unit and or branch manages its assets. Risk is a key component of strategic asset management and, as such, business areas will maintain key asset risk within the divisional risk profiles.	Continual monitoring	Asset Managers and Owners
Security and emergency management	Risk assessments of TCCS sites and enterprise security risk reviews are outsourced to specialist service providers and managed by the Security and Emergency Management team. Enterprise security risk reviews and site assessments are undertaken to support identification of critical assets and the potential security vulnerabilities. Further information on managing security risks, enterprise security risk reviews and site assessments is available in the TCCS Protective Security Policy. Key security risks will be maintained within divisional risk profiles.	Continual monitoring	Security and Emergency Management Team
Fraud and corruption prevention	Suspected fraud and corruption is actively managed within TCCS, with a designated executive responsible for documenting and investigating fraud and corruption issues. The Senior Executive Responsible for Business Integrity Risk (SERBIR) is to be informed of any fraud and corruption related matters (suspected or otherwise). A directorate level fraud risk assessment is developed and maintained in accordance with the TCCS Fraud and Corruption Prevention Plan. Fraud risk is to be managed by nominated risk owners.	6 Monthly	SERBIR/ Risk Owners
Financial risk management	In order to effectively manage Financial risk, TCCS have established a Finance Committee to provide leadership and direction in financial strategy and financial management of the Directorate. A key responsibility of the committee is to oversee the development of budgetary and financial management implications in relation to governance and risk management structures and processes, aligning with the work of the Internal Audit Committee. Membership includes key TCCS Executive staff.	Continual monitoring/ Quarterly meetings	CFO/Finance Committee

	TCCS works collaboratively with the ACT Audit Office to undertake financial audits to investigate financial statements and statements of performance. TCCS will continue to assist the ACT Audit Office by presenting a true and fair view of their financial results and operating performance.		
Program and project risk	In delivering projects and programs, TCCS personnel are required to effectively identify, control, treat and monitor risks. Risk management is embedded into the TCCS project/program management process and is a consideration of all phases the project lifecycle. Program and project risks are to be managed by TCCS and these must be incorporated into the project plan. These identified risks are monitored and reported through project plan specific risk governance mechanisms, such as steering committees, or executive sponsored working groups. The Project Management Office (PMO) offers support to TCCS projects by providing gate reviews of projects and programs. The PMO uses a systematic approach to support monitoring progress of the project or program to control risk and cost.	As Required	Project/ Program Team and/or Project Steering Committee
Procurement and contract management risk	Procurement, contract management and contract administration risk is managed using various methods ranging from completing a risk assessment questionnaire for low dollar and low risk procurements through to a risk management plan for procurements of high risk and procurements where the value is more than $5 million. Procurement risk will be managed dependant on the guidelines in which TCCS is undertaking procurement activities. The procurement and contract management assurance framework provides a checklist for assessing procurements are being conducted in accordance with agreed policies and procedures. Key contract risks will be maintained within divisional risk profiles. Assurance will be gained through compliance reviews and audits.	As required	Program/Project and/or Contract Managers

Workplace health and safety risk	*Work Health and Safety Act 2011* requires employers to provide and maintain a safe workplace and safe systems of work. TCCS has proactive risk assessment and workplace health and safety policies, strategies, and procedures in place to actively promote workplace health and safety and minimise accidents and injuries. Systems used to reduce risk:
	• Work Health and Safety Management System (WHSMS) – SafetyNet.
	  ○ Hazard and incident reporting (Riskman).
	  ○ Transport Canberra Incident Management System (IMS).
		6 Monthly	Executive Branch Manager Safety and Wellbeing/ Risk Owners

Regulatory and legislative compliance	The Head of Service established the ACT Public Sector Compliance Project in 2019 to provide oversight and specialist advice to ensure Directors-General and other senior Executives are aware of and have arrangements and resources in place to ensure compliance with their legislative and non-legislative obligations. TCCS are committed to implementing the whole of government project, which will	Project Implementation plan in place	COO/ EBM GAMS

	encompass both delegations and applying risk management within the regulatory and legislative environment.		
TCCS Quality Management System	TCCS has established a quality management system by establishing, implementing, maintaining, and continually improving, including processes needed and their interactions, in accordance with ISO9001:2015, including addressing risks and opportunities.	Continual monitoring	COO/ EBM GAMS
Audit, assurance, and testing activities			
Quality management	Business areas are to implement quality management systems in accordance with the TCCS Quality Management Policy and Framework. This includes implementing quality assurance processes to test compliance with procedures, risk identification and continuous improvement.	Continual monitoring	Quality Team
Internal audit function – assurance program	The internal assurance program is developed in consultation with the Executive Leadership Team, endorsed by the TCCS Audit Committee. Whole of Directorate strategic risks, high profile division and business unit risks, control and treatments as identified in the applicable risk registers, are a thoroughly assessed for better practice outcomes. Audit activities include Audits undertaken by an independent audit provider.	Forward Annual Plan	Audit and Risk Team
Insurable Risk			
ACT Insurance Authority (ACTIA)	ACTIA is tasked under the *Insurance Authority Act 2005* with promoting the adoption of good risk management practices throughout all ACT Government directorates and organisations. The ACT Government and TCCS use the internationally accepted standard AS/NZS ISO 31000 as the basis for best practice risk management within the Territory. ACTIA provides cover to the Directorate for all normally insurable risks and where applicable project specific risks (which may be covered through a Project Agreement between the Territory and identified party). Cover provided by ACTIA for the directorate includes: • property and physical assets; • public and product liability; • professional indemnity; • board directors' and officers' liability; and • volunteer personal injury and liability.	Asset and Non-Asset declarations are provided to ACTIA annually Potential Claims against the Territory as required	Business areas

Appendix C: Risk Glossary

Term	Definition
ACT Insurance Authority (ACTIA)	ACTIA is tasked under the *Insurance Authority Act 2005* of promoting the adoption of good risk management practices throughout all ACT Government directorates and organisations. Risk management initiatives promoted by ACTIA include but are not limited to: • Promotion of risk management forums and networking meetings for ACT Government personnel involved in risk management; • Assisting directorates with the development of their risk management programs, policies and practices; • Provision of a variety of risk management and insurance training courses for Directorate representatives; • Provision of risk management tools; • Provision of assistance to directorates in identification, assessment, and treatment of risks for all activities managed by the Territory.
Audit Committee	The *Financial Management ACT (FMA) 1996* states that an audit committee is appointed to oversee and advise the directorate on matters of accountability an internal control.
Consequence	The impact or impacts a risk event will have on objectives if it occurs.
Control	A measure that has a modifying effect on risk. A risk control can include processes, policies, devices, practice, or other actions that are designed to modify risk.
Control Effectiveness	**Adequate** – Controls are well designed and operating effectively in treating the cause of the risk. Additional controls exist to appropriately manage consequence. No further treatments is required except to review and monitor existing controls. Controls are largely preventative, and management believes that they are always effective and reliable. **Room for Improvement** – Some deficiencies in controls have been identified however most controls are designed and implemented effectively in treating some root causes of the risk. While some preventative controls exist, they are largely reactive. There are opportunities to improve the design/implementation of some controls to improve operational effectiveness. **Inadequate** – Significant control deficiencies are identified. Either controls do not treat the root cause, or they do not operate effectively. Controls, if they exist are just reactive. Management has little confidence on the effectiveness of the controls due to poor control design and/or very limited operational effectiveness.
Corrective control	These are reactive controls put in place to reduce the consequence of an eventuated risk e.g., Business Continuity Plans, Insurance.
Detective Control	These are proactive controls put in place to check the likelihood of a risk eventuating e.g. verifications, reviews, desktop audits.

Event	Occurrence of or change of a particular set of circumstances. Note 1: An event can be one or more consequences and can have several causes. Note 2: An event can consist of something not happening. Note 3: An event can sometimes be referred to as an "incident" or an "accident".
Inherent Risk	The current or original risk rating which considers current controls prior to the addition of risk treatments.
Level of Risk	Magnitude of a risk or combination of risks expressed in terms of the combination of consequences and their likelihood. (May also be referred to as risk severity)
Likelihood	Chance of a risk being realised.
Preventative Control	These are proactive risk controls put in place to reduce the likelihood of a risk eventuating e.g., monitoring, approvals, and compliance reviews
Program	A program manages a set of related projects and/or activities in order to deliver outcomes and benefits related to organisational objectives. A program may have a lifespan of several years during which a number of projects are initiated, executed, and closed. The program co-ordinates the interdependencies amongst the various projects and activities to deliver an outcome greater than the sum of its parts.
Project	A project is a temporary one-time effort to achieve explicit objectives within defined time, cost, and performance parameters. The project brings about change and involves a group of inter-related activities that are planned and then executed in a certain sequence to create a unique product, service, undertaking or result within a certain timeframe.
Residual Risk	Risk remaining after a risk treatment has been implemented.
Risk	Effect of uncertainty on objectives.
Risk Appetite	Amount and type of risk that an organisation is willing to pursue or retain.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Criteria	Terms of reference against which the significance of a risk is evaluated.
Risk Description	Structured statement of risk usually containing four elements: sources, events, causes and consequences.
Risk Identification	Process of finding, recognising, and describing risks.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk. i.e., from management policies, procedures, and practices to the tasks of establishing the context, analysing, evaluating, treating, monitoring, and communicating risk
Risk Management Framework	The set of components needed to design, implement, and operate an effective risk management system.

Risk Management Plan	A document that specifies the approach, tasks, and assignment of responsibilities to be applied to the management of risk affecting an aspect of the ACT Government's business.
Risk Matrix	Tool for ranking and displaying risks by defining ranges for consequence and likelihood.
Risk Management Standard AS ISO 31000:2018	The Standard is a generic and flexible standard that is not specific to any government or industry sector. The Standard identifies elements or steps in the risk management process that can be applied to a wide range of activities at any stage of implementation.
Risk Owner	Person or entity with the accountability and authority to manage risk. In the ACT Government context this is the officer/manager who has the authority to manage the risk.
Risk Profile	Identifies, assesses, and evaluates key risks facing the enterprise against a number of facets including probability and impact. The risk profile understands how risks are identified, measured, and managed, and how these processes are integrated into an overall risk profile. **Note:** the set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined.
Risk Register	Documented record of information about identified risks. A risk register is the tool used to record the results of the risk assessment.
Risk Source	Element which alone or in combination has the intrinsic potential to give rise to risk.
Risk Strategy	A high-level statement that sets out the broad policy as to how risk will be taken and managed by the organisation to achieve its strategic objectives. The risk strategy defines the way in which an organisation undertakes risk management, and aids decision making and the effective use of scarce resources.
Risk Treatment	Process of selection and implementation of measures to modify risk (with aim to reduce or eliminate risk).
Risk Treatment Owner	The officer/manager responsible for managing the treatment of risks. This includes ensuring that the treatment strategy outlined is implemented and is doing what it was designed to do – manage the risk.
Risk Treatment Action Plan	A document that supports identified risks detailing strategies and actions for how Branch/Business Unit plans to respond to the potential risk.
Riskware	A cloud-based Enterprise Risk Management system that is a registered trademark developed by Pan Software.
Stakeholder	Any person and/or entity / organisation that has the ability to influence the organisation's ability to meet their objects and /or is affected by the organisation's decisions or activities. A stakeholder includes individuals and entities that perceive themselves to be affected by a decision or activity.