CULTURAL FACILITIES CORPORATION
RISK MANAGEMENT PLAN

Authorised by :	Harriet Elvin Chief Executive Officer Cultural Facilities Corporation
Date :	8 December 2021
Board approved :	*8 December 2021*
Date for review :	*November 2023*
Version :	Version 1.0

DOCUMENT CONTROL

Prepared for	Cultural Facilities Corporation
Document Owner	Chief Finance Officer/ Senior Executive Responsible for Business Integrity Risk
File Name	CFC Risk Management Plan
Version	1.0
Status	Draft

Revision

This Risk Management Plan must be reviewed and updated every two years (or more frequently following major change to business operations and/or priorities) as a part of Cultural Facilities Corporation business planning process.

Revision	Description	Date	Author
0.1	Initial draft	Nov 2021	Chief Finance Officer/ Senior Executive Responsible for Business Integrity Risk
1.0	Final	Nov 2021	Chief Finance Officer/ Senior Executive Responsible for Business Integrity Risk

Review and authorisation

The Risk Management Plan is to be reviewed and endorsed by the Chief Executive Officer, Cultural facilities Corporation.

This is an Open Access Document.

Harriet Elvin AM
Chief executive Officer
Cultural Facilities Corporation

Date 8 December 2021

INTRODUCTION

Purpose

The Cultural Facilities Corporation (CFC) is committed to the effective and efficient identification, treatment and monitoring of risks to the organisation. Oversight of risk management processes are undertaken by the CFC Board, CFC Audit Committee, and the Senior Management team.

The CFC aims to pursue an effective risk management philosophy and culture through a governance framework with a fully integrated Risk Management Plan (the Plan).

The objectives of this Plan are to:

- provide a detailed guide to support the effective implementation of the CFC Risk Management Framework and Policy;
- outline the risk management process to be followed by the CFC;
- minimise the CFC's exposure to significant risks through the identification; assessment, management, monitoring, review and reporting of risk; and
- enhance the CFC's ability to capitalise on opportunities through minimising risk and improving overall performance.

Robust risk management practice outlined and supported by this plan will enable:

- consistent, confident and accountable planning and decision-making;
- confident 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;
- the anticipation or prediction of future occurrences, recognising external factors that may impact the organisation;
- excellence in management, encouraging innovation that includes responsible risk taking;
- forward thinking and active approaches to management rather than reactive management;
- effective allocation and use of resources;
- sound incident management and reduction in the cost of risk, including insurance and worker's 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;
- 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 to be realised between the cost of managing risk and the anticipated benefits.

Scope

The Plan establishes the processes for risk management in CFC. It seeks to minimise exposure to significant risks through the identification, assessment and management of risk, as well as to enhance the ability to capitalise on opportunities through minimising risk and improving overall performance.

The risk management process is designed to ensure that risk management decisions are based on a robust approach, assessments are conducted in a consistent manner, and a common language is used and understood across the CFC.

This Plan is consistent with the AS ISO 31000:2018 Risk Management – Principles and Guidelines standard ("the Standard"). Territory entities must ensure that they comply with this Standard.

Tools

The CFC has several documents and tools for conducting risk assessments and the ongoing management of risk.

Table 1 – Risk Management Tools supporting the risk assessment process

Tool	Description
Risk Register Template	The Risk Register enables staff to document, manage, monitor, review and update strategic and operational risk information. For each risk, the following will be captured: • the risk category • a description of the risk event • the cause or source of the risk • the nature and extent of the expected consequences associated with the risk • the likelihood of the expected consequences • the name(s)/position(s) of the risk owner(s) • the existing controls being relied upon • the name(s)/position(s) of the control owner(s) • the control effectiveness (CE) • the risk rating
Risk Treatment Action Plans	Information from the risk management process is recorded, reported and monitored using the Risk Register. A Risk Treatment Action Plan will be prepared for all 'high' and 'extreme' rated risks. Risk Treatment Action Plans will contain: • the tasks to be completed and the risks they address • the name/position of the task owners who have responsibility for implementation of treatment tasks • the timetable for implementation or next review date for the treatment implementation process.
Shared Drive	Access to policy, guidelines and template documents through the G:CFC/Staff share drive.

Tool	Description
Training	Ongoing training and development for relevant team staff to ensure that the team is equipped with sound risk management knowledge and skills base. Contact the CFC HR Manager, for further information or to book relevant training.
Reporting	*Refer to Reporting section following for details.* Risk reports draw information from the risk registers and allows management to monitor and review risks in alignment with the strategic plan, operational plans, programs of change and other cascading plans.

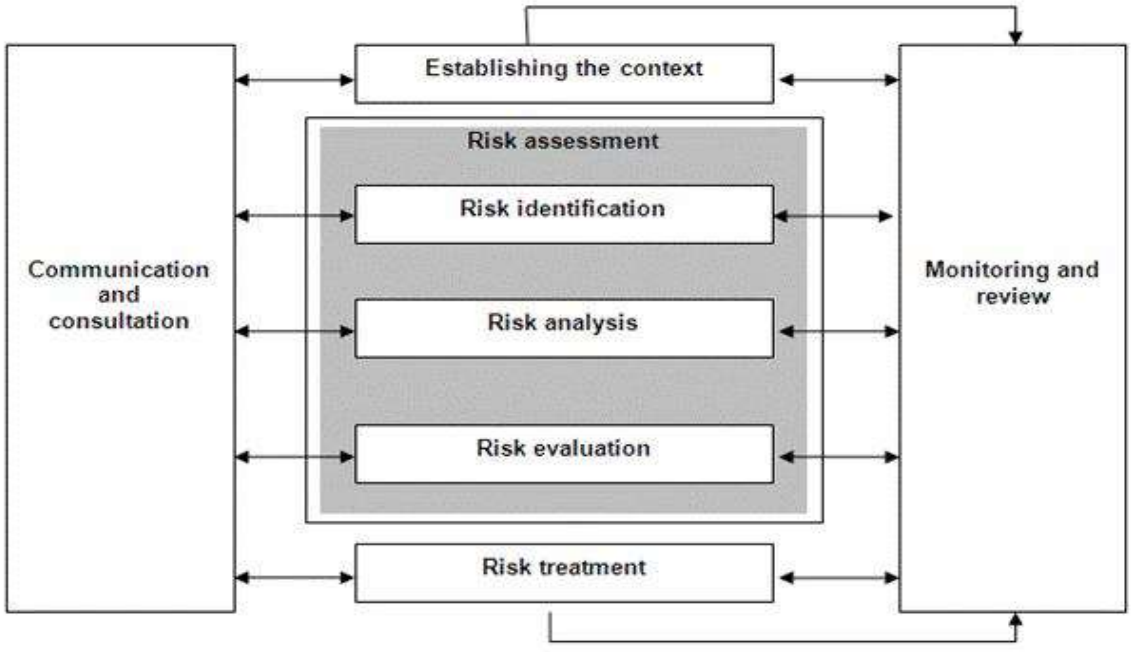
RISK MANAGEMENT PROCESS

Risk management is a repetitive process of continuous improvement that is best integrated into existing practices and business processes. To be effective, robust risk management practice should become embedded into the organisational culture of CFC and risks should be managed according to the CFC Risk Management Framework and Policy and 'The Standard' upon which this document has been built.

The elements of the risk management procedures and practices require the following key processes:

1. communication and consultation;
2. establishing the context;
3. risk assessment (including identification, analysis and evaluation);
4. risk treatment; and
5. monitoring and review.

Diagram 1 – The risk management process as set out in the AS ISO 31000:2018 risk management standard



RISK ASSESSMENT – DEVELOPING RISK REGISTERS

1. Communication and Consultation

Effective communication, consultation, engagement and education in risk management are necessary to achieve successful integration of the risk management process in CFC to achieve the overall objectives of the Agency.

To ensure that this is achieved it is important that everyone affected by or likely to influence the subject of a risk assessment is included in the process. From the earliest opportunity, two-way communications with all stakeholders (internal and external) will ensure the most effective outcomes and support the risk management process.

The purpose of communication and consultation is to ensure that:

- the context is appropriately defined;
- staff are involved and therefore understand the basis for decisions and actions required;
- stakeholder perceptions of risk have been addressed; and
- lessons learnt are shared and transferred to those who can benefit from them.

This step should be repeated throughout the risk management process.

2. Establishing the Context

The process of establishing the context defines the basic parameters for managing risks and sets the scope for the application of the risk management process. It is an important step that if overlooked or trivialised may result in an ineffectual risk assessment. Establishing the context is the process of:

- Articulating and defining both the internal and external factors influencing the ability to achieve objectives;
    - *External factors* - social and cultural, political, legal, regulatory, financial, technological, economic, natural, and competitive environment
    - *Internal factors* – governance, organisational structure, policies, strategies, available resources, information systems, decision-making processes.
- Determining the boundaries within which the risk management framework operates (consider goals and objectives, methodologies, relationships/dependencies with projects, processes and resources).
- Defining risk criteria to ensure risks are assessed in a consistent manner. ACT Government and accordingly CFC has established its risk criteria and they are contained in Attachment A ACT Government Risk Assessment Matrix.

Thorough consideration of the risk management context will help to ensure that, opportunities to achieve organisational objectives are exploited and innovative solutions to address identified risks are not overlooked.

3. Risk Assessment

The risk assessment component of the risk management process has three key components – identification, analysis and evaluation of risks.

3.1 Risk assessment - Step 1. Risk Identification

Risk identification is the *"process of finding, recognising and describing risks*[1]*"* It is important that all the risks which relate to your activity are identified. As stated in the Standard, *"comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis."*

Risk identification generates a comprehensive list of threats and opportunities based on those events that might enhance, prevent, degrade, accelerate or delay the achievement of objectives. The results of the identification process are recorded as the risk description and include the risk event, its sources and causes and the potential consequences.

Risk descriptions should aim to be structured and systematic in that, sources/causes and consequences are easily aligned to identify potential gaps in processes. (This also should be a key consideration when articulating controls.)

3.2 Risk assessment - Step 2. Risk Analysis

Risk Analysis is the *"process to comprehend the nature of risks and to determine the level of risk. Risk Analysis provides the basis for risk evaluation and decisions about risk treatment.*[2]*"*

The analysis of risk generally involves consideration of the risk event, the range of causes and sources of the risk, the current controls, the effectiveness of the current controls (do the controls have the intended modifying effect), the "consequence" to the organisation and the "likelihood" of it happening. The level of risk arrived at is referred to as the 'inherent risk rating' or the current risk rating.

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	High	Extreme
Possible	Low	Medium	Medium	High	Extreme
Unlikely	Low	Medium	Medium	High	High
Rare	Low	Low	Medium	Medium	High

3.3 Risk assessment - Step 3. Risk Evaluation

Risk evaluation compares the risk analysis with the risk criteria to determine whether the risk is acceptable or tolerable. Risk evaluation determines if controlled risks need further treatment and identifies priority order in which individual risks should be treated.

[1] ISO Guide 73:2009

[2] ISO Guide 73:2009

4. Risk Treatment

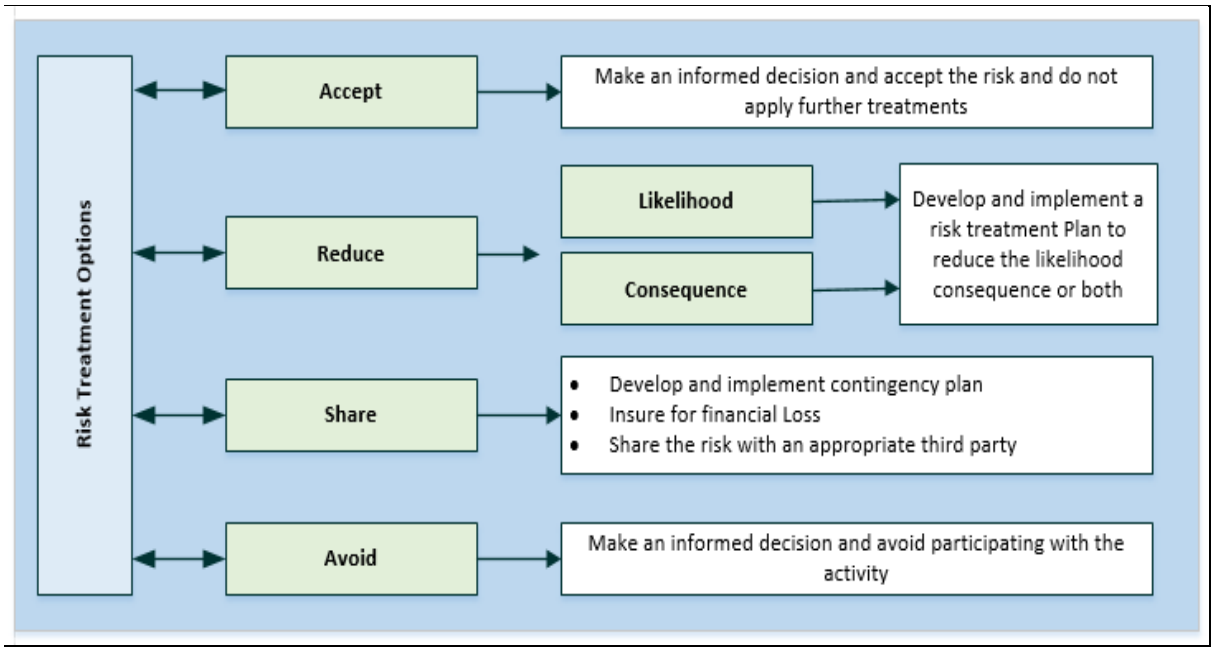
Treatment of risk involves selecting one or more options for modifying the risk or managing the risk to a status acceptable within the Agencies risk tolerance. This will generally include developing and implementing specific strategies and action plans for increasing potential benefits and improving outcomes to better manage the risk. To improve the management of controls and treatments the use of SMART methodologies is recommended. It should be noted that not all treatments can have it applied.

- Specific (simple, sensible, significant).
- Measurable (meaningful, motivating).
- Achievable (agreed, attainable).
- Relevant (reasonable, realistic and resourced, results-based).
- Time bound (time-based, time limited, time/cost limited, timely, time-sensitive).

By using the SMART methodology, it will provide you with a mechanism to test the control and report to the risk owner the effectiveness of the control.

Risk treatment recognises that elimination of risk is not always possible or desirable aiming instead to drive the risk as low as is reasonably practicable or achievable thereby achieving a balance between the cost of managing the risk and the anticipated benefits. Risk is then reassessed providing an assessment of the residual risk – the level of risk with controls and treatments in place.

The below table outlines potential risk treat mechanisms.



5. Monitoring and Review

The risk management process is repetitive and should be the subject of a structured monitoring and review process. Regular monitoring and review of the risk assessment will:

- determine whether the risk profile has changed and whether new risks have emerged;
- provide feedback on control efficiency and effectiveness or test the effectives of current controls;
- track the progress of risk treatment actions;
- identify whether any further treatment is required;
- provide a basis to reassess risk priorities; and
- capture lessons learned from event failures, near misses and success.

The following diagram illustrates the ongoing nature of risk management and how it applies within CFC. The processes set out in the AS ISO 31000:2018 Risk Management Standard have been represented in a continuous cycle, as risk management is not a static activity. Communication and consultation are represented as a fundamental principle applied at all stages of the risk assessment process. Additionally, the CFC's reporting and recording processes have been built into the model to support the requirements of escalation and reporting of risks and maintenance of our records.

6. Reporting

Risk register reporting allows the monitoring, reviewing and reporting of risks in alignment with the strategic plan, operational plans, programs of change and other cascading plans.

As there is no one single risk report that meets the decision-making needs of an organisation, risk reports are to be tailored by the accountable area to support management decision making during the planning and review processes.

Risk reports draw information from the risk registers and, depending upon the requirements, may include:

- a demonstration of the link between objectives and risks;
- priorities, based on the risk rating, accompanied by information on key controls and treatments needed to modify the risk;
- risks that are getting worse, success of treatment plans and risks that require additional attention;
- new risks that may still need to be fully considered and understood;
- potential areas that require urgent attention;
- main areas of exposure;
- systemic control analysis;
- untreated risks and risk treatments that are overdue; and
- risk owners.

7. Recording and Maintenance

All risk management documentation is to be recorded, stored and maintained in an appropriate manner.

Risk registers should be reviewed annually or as determined as part of the business and strategic planning process.

Programs and Projects are to conduct reviews of existing risks on a regular basis in accordance with normal program management requirements – set out in the risk management plan that relates to the program.

Risk owners will have accountability and authority for managing the risk and managing the owners of any associated risk treatments.

ACTIVITIES SUPPORTED BY THIS RISK MANAGEMENT PLAN

Risk management is an overarching principle that, when conducted effectively, supports an organisation to achieve its objectives and maximise opportunities. Activities supported by this risk management plan include the following:

Strategic Risk Management Register

High level risks facing the CFC are identified in this Register, together with appropriate treatments. This allows the Board, Audit Committee, and Senior Management team to focus on strategic risk management.

Internal Audit

The Internal Audit Program and CFC's Quality Assurance program have been developed in part based on the Strategic Risk Register and CFC Risk Registers with a view to testing and validating the Risk Registers and Plan to ensure that treatments and controls are adequate.

Business Continuity Management

Business continuity management, or the management of disruption related risk, is a risk treatment. Business continuity management and business continuity planning (BCP) activities are designed to reduce the consequence(s) of a business interruption event.

Business continuity management involves the following key steps:

- a business impact analysis;
- development of response strategies;
- identification of resource requirements; and
- development of Business Continuity Plans.

The purpose of the BCP is to outline arrangements in place to ensure continuity of the organisation's key services after a major, unexpected and disruptive incident that causes interruptions to the delivery of the organisation's services. Such interruptions might include problems associated with accommodation, information and communications technology and personnel. The BCP analyses and records potential business impacts, recovery priorities and risk management strategies. It also describes the management structure, staff roles and responsibilities, and actions that are to be implemented after a major incident. BCPs will be tested on a regular basis to ensure their effectiveness.

The CFC Senior Management team is responsible for coordinating the development, monitoring, testing and review of the CFC BCP documentation.

Fraud and Corruption Prevention

A key risk for any organisation is fraud and corruption. CFC has a Fraud and Corruption Prevention Plan and Policy and an associated Fraud Risk Register.

Integrity risk is an important subset of business risk. Integrity risks are those actions or omissions that put at risk the resources, assets, security and reputation of the Territory and/or its agencies. The CFC Fraud and Corruption Prevention Plan and Policy aims to enhance integrity, reduce the risk of fraud and corruption, as well as assist staff to make

decisions in the reporting of fraud, corruption and other criminal offences affecting the organisations.

The fraud and corruption risk assessment, evaluation and planning processes are ongoing management responsibilities. Fraud and integrity risks should be identified as part of the overall risk management processes contained in this policy.

Senior Executive Responsible for Business Integrity Risk (SERBIR)

In accordance with the *Public Sector Management Act 1994* and the ACT Integrity Policy the Chief Executive Officer is required to appoint a Senior Executive to take responsibility for all integrity issues within each organisation. The Senior Executive Responsible for Business Integrity Risk (SERBIR) for CFC is the Chief Finance Officer. The SERBIR is a 'champion' of integrity in CFC and promotes awareness and acceptance of the ACTPS Integrity Policy and the CFC's Fraud and Corruption Prevention Plan and Policy. The SERBIR is also responsible for regularly reporting on overall compliance with the relevant policies to the Chief Executive Officer, Senior Management team and the Audit Committee.

Workplace Health and Safety

The CFC values staff, contractors, customers and the environment in which we operate our business. As such work, health and safety (WHS) is a priority.

The Work Health and Safety Act 2011 requires employers to provide and maintain a safe workplace and safe systems of work. Workplace safety awareness and robust risk management practice aims to ensure that our workplaces are safe thus reducing incidents of death, injury and disease.

CFC 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.

This risk management plan provides the processes for risk management that applies in the context of work, health and safety. Risks relating to work, health and safety and the protection of people should be considered when undertaking risk assessments. A risk register that outlines how we have identified risks relating to work, health and safety, the current controls in place, analysis of the risk, evaluation and prioritisation for treatment, monitor and review of the risks and implementation of identified risk treatments should be maintained to meet CFC's obligations.

Training and Support

This Plan, in conjunction with the CFC Risk Management Framework and Policy, are intended to assist staff and managers understand their roles and responsibilities in relation to risk management. To ensure consistent, appropriate application of the risk framework and policy and to increase risk management maturity across CFC, regular risk management training is made available to all staff. CFC HR will manage and support training that includes Fraud Prevention awareness training in addition to risk management training. Additional risk management training may be accessed by staff through the ACT Government training calendar and by the ACT Insurance Authority.

ATTACHMENT A – PART 1 – ACT GOVERNMENT RISK ASSESSMENT MATRIX

Likelihood	Frequency			Consequence					
					Insignificant	Minor	Moderate	Major	Catastrophic
				Matrix	1	2	3	4	5
	Almost Certain	Occurs on most occurrences of the activity	Expected to happen this time	**5**	**Medium**	**High**	**High**	**Extreme**	**Extreme**
	Likely	Occurs on some occurrences of the activity	Expected to occur on one of the next few occasions	**4**	**Medium**	**Medium**	**High**	**High**	**Extreme**
	Possible	Infrequently occurs here	Could occur at some time in the future. Would not be surprised if it occurred.	**3**	**Low**	**Medium**	**Medium**	**High**	**Extreme**
	Unlikely	Has never occurred here	Might occur but unlikely. Would be surprised if it occurred.	**2**	**Low**	**Medium**	**Medium**	**High**	**High**
	Rare	Has never occurred here, but may have/has occurred somewhere	Might occur, but only in exceptional circumstances. Would be very surprised if occurred.	**1**	**Low**	**Low**	**Medium**	**Medium**	**High**

		Priority for Attention/Action	
	Indicative escalation	Suggested timing for treatment	Authority for tolerance of risk
Extreme	Within 24 hours	Short-term – normally within one month	CEO
High	Within 14 days	Medium-term – normally within three months	Senior Management team
Medium	Within 1-3 months	Normally within one year	Managers
Low	1-3 months in course of normal business	Ongoing control as part of a management system	All Staff

Risk Control Effectiveness	
Control Effectiveness	**Guide**
Adequate	Controls are well designed and operating effectively in treating the root cause of the risk. Additional controls exist to appropriately manage consequences. Controls are largely preventative, and management believes that they are effective and reliable at all times. Nothing further to be done except review and monitor existing controls.
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, controls are largely reactive. There are opportunities to improve the design/implementation of some controls to improve operational effectiveness.
Inadequate	Significant control deficiencies 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 of the effectiveness of the controls due to poor control design and/or very limited operational effectiveness.

		Consequence of risk in the most normal form				
Category of Risk	**Contextual definition**	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Business Operations	Achievement of strategic and operational business objectives	Minor errors in systems or processes requiring corrective action and/or minor delay without impact on overall schedule and/or insignificant impact on business outcomes and strategic objectives.	Services (including those of providers) do not fully meet needs and/or minor impact on business outcomes and strategic objectives and/or subsidiary services experience minor disruptions.	One or more key accountability requirements not met and /or inconvenient but not client welfare threatening and/or moderate impact on business outcomes and strategic objectives and/or a number of objectives not met, minor or subsidiary services impaired.	Significant impact on business and / or strategic objectives and/or strategies not consistent with Government's agenda and/or trends show service is degraded and/or key service delivery impaired.	Strategic business outcomes/ processes fail, control infrastructure failure, critical business objectives not met.
Service Delivery	Delivery of functions of the business/branch/ entity depending on their classification as essential/critical or not	No loss of an essential/critical service and/or loss of, or interruption to, non critical/non-core services up to 3 days.	Loss of an essential/critical service for less than 4 hours and/or loss of, or interruption to, non critical/non-core services for 3 - 5 days.	Loss of one or more essential/critical services for more than 4 hours and up to 3 days, and/or loss of, or disruption to, non critical/non-core services for up to 10 days.	Loss of one or more essential/critical services for more than 3 days and up to 4 or more weeks, and/or loss of part of an essential service that is high risk (life based) and/or disruption to non-critical services over subsequent weeks.	Loss of one or more essential/critical services for more than 4 weeks that continues for months and/or loss of an essential service that is high risk (life based) and/or disruption to non-critical services over subsequent months.
Compliance/Regulation	Non compliance with legislation, regulation, policy or procedure (including conflicts of interest), and the associated consequences to operations	Non-compliance with policies, procedures & guidelines and standard operating procedures which are not legislated or regulated.	Numerous instances of non-compliance with work policy and standard operating procedures which are not legislated or regulated.	Non-compliance with work policy and standard operating procedures which are regulated or legislated.	Restriction of business operations by regulator due to non-compliance with relevant guidelines and / or significant non-compliance with policy and procedures which threaten business delivery.	Operations shut down by regulator for failing to comply with relevant guidelines / legislation and /or significant non-compliance with internal procedures which could result in failure to provide business outcomes and service delivery.
Cultural & Heritage	Damage or adverse outcomes to items or places of cultural or heritage value	Consists of, but is not limited to, repairable damage or no impact to the heritage place or object and/or Unauthorised conduct to the heritage place or object, including Aboriginal places and object. The conduct has no or repairable impact.	Consists of, but is not limited to, repairable damage to the heritage places or object and/or Unauthorised conduct that diminishes the heritage significance of the place or object, including Aboriginal places and objects. The conduct has minor repairable adverse heritage impact.	Consists of, but not limited to, repairable or irreparable damage to the heritage place or object and/or Unauthorised conduct that diminishes the heritage significance of the place or object, including Aboriginal places and objects. The conduct may or may not have an acceptable heritage impact.	Consists of, but not limited to, significant, or irreparable damage, or total loss of the heritage place or object and/or Unauthorised conduct, including negligent conduct, that diminishes the heritage significance of the place or object, including Aboriginal places and objects. The conduct has an unacceptable heritage impact.	Consists of, but not limited to, permanent or irreparable damage, or total loss of the heritage place or object and/or Unauthorised conduct, including reckless conduct, that diminishes the heritage significance of the place or object, including Aboriginal places and objects. The conduct has an unacceptable heritage impact.
Financial	Financial losses from the project or entity represented as either a percentage of the project/entity budget or a dollar amount, which ever is the greater	1% of Project / Entity Budget or <$5K	2.5% of Project / Entity Budget or <$50K	> 5% of Project / Entity Budget or <$500K	> 10% of Project / Entity Budget or <$5M	>25% of Project / Entity Budget or >$5M
Information & Records Management	Access to and security of information and records that enable the conduct of business and provision of services	A product or service which services up to 10% of the workforce or impacts a small number of the community in a minor way and/or System breach to business administration system with no personal or classified information stored.	A product or service which services 10 - 30% of the workforce or impacts a small number of the community in a moderate way and/or System breach to business administration system with some identifiable information but non-client threatening (data access known).	A product or service which services 30-70% of the workforce or impacts a moderate number of the community in a moderate way and/or System breach to business administration system with some identifiable information but non-client threatening (data access unknown).	A product or service which services greater than 70% of the workforce or impacts a small to moderate number of the community in a major way and/or Systems breach to business administration system with identifiable/classified information stored but non-client welfare threatening.	A product or service which services 100% of the workforce or impacts a moderate or substantial number of the community in a major way and/or total loss of confidence in data/record integrity and/or Systems breach to Government or business critical systems with client and/or business welfare threatened.
Natural Environment	Adverse outcomes for the natural environment	Environmental harm to an ecosystem and species is limited to a localised area with rapid recovery without effort.	Minimal environmental harm to an ecosystem and species recognised at the local or regional level and/or Localised but minor instances of environmental harm that can be reversed with minimal efforts.	Moderate environmental harm to an ecosystem and species recognised at the state level and/or Semi-permanent loss of environmental value and risk of continuing environmental harm.	Major environmental harm to an ecosystem and species recognised at the national level and/or Loss or impairment to an ecosystem or species recognised at the state or regional level and/or Difficulty recovering from environment damage and stemming ongoing environmental harm.	Severe Damage and/or significant loss and/ or impairment and/or Permanent destruction of an ecosystem or species recognised at the local, regional, state or national level and/or Permanent and widespread loss of environmental value and progressive irrecoverable environmental harm.
People Injuries (physical & psychological)	Direct physical and psychological injuries to people (staff, contractors, customers) arising from the risk occurring. The impact to people arising from Natural Disaster related events is covered under the Emergency / Disaster Management categories	No injury or treatment required.	Injury which: •requires treatment (not hospitalisation); and/or •impacts capacity to work for a period of one week or less; and/or multiple people sustain injury/ies not requiring treatment.	Injury which: •requires hospitalisation; and/or •impacts on capacity to work for a period of greater than one week; and/or multiple people sustain injury/ies which: •require treatment •impact their capacity to work for a period of one week or less.	Single injury which: •is life-threatening (including loss of limbs); and/or •results in permanent disability; and /or •results in permanent (partial or total) impact on capacity to work; and /or multiple people sustain injury/ies which: •require hospitalisation •impact their capacity to work for greater than one week.	Death and/or multiple injury/ies which result in: •permanent impact on capacity to work; and/or •permanent disability.
Reputation & Image	Observable measures of how the risk may impact the reputation or image of the ACT Government	Internal review and/or minor dissatisfaction across a small number of demographic groups or stakeholders.	Scrutiny required by internal committees or internal audit to prevent escalation and/or moderate dissatisfaction across a small number demographic groups or several stakeholders.	Local media scrutiny (1 week) and/or scrutiny required by external committees or ACT Auditor General's Office, or inquest, etc and/or dissatisfaction across a few demographic groups or multiple stakeholders.	Intense public, political and national media scrutiny (1 week) and/or Minister / Chief Minister involvement and/or dissatisfaction across a large range of demographic groups and stakeholders.	Adverse finding from Assembly inquiry or Commission of Inquiry or sustained adverse international media and/or loss of public confidence in Government or Public Service forcing changes to the machinery of Government.
Emergency / Disaster Management (social impact)	Measures of the social impact to the ACT arising from emergencies (eg bushfire, flood, storm damage etc)	The community's social connectedness is disrupted, such that the reprioritisation and / or reallocation of existing resources is required to return the community to functioning effectively, with no permanent dispersal.	The community's social connectedness is disrupted, such that community requires some external resources to return the community to functioning effectively, with no permanent dispersal.	The community's social connectedness is disrupted, such that community requires significant external resources to return the community to functioning effectively, with some permanent dispersal.	The community's social connectedness is significantly disrupted, such that extraordinary external resources are required to return the community to functioning effectively, with significant permanent dispersal.	The community's social connectedness is irreparably disrupted, such that the community ceases to function effectively, breaks down and disperses in its entirety.
Emergency / Disaster Management (community / people impact)	Outcomes on the community or people of the ACT arising from emergencies (eg bushfire, flood, storm damage etc).	Minor injuries to 10 or less people.	Less than 4 serious injuries, or more than 10 minor injuries directly from the emergency.	Less than 4 deaths or critical injuries with long-term or permanent incapacitation, directly from the emergency, or more than 4 serious injuries.	4 – 40 deaths or critical injuries with long-term or permanent incapacitation, directly from the emergency, or more than 40 serious injuries.	More than 40 deaths or critical injuries with long-term or permanent incapacitation, directly from the emergency.

Climate Change	The consequences of a changing climate are inherent to many of the consequence categories listed and may be considered as part of a risk assessment. For example, frequent heatwaves may risk damage to physical assets, which may create financial risks, inability to deliver core services, negatively impact the government's reputation and reduce general business activity etc.
Essential Services	Definition of an essential service: Essential services may take two forms – those which are public facing and those which are internal and necessary for the ongoing business of government, such as support to Ministers, making payments to providers and suppliers, and supporting the workforce. Government have determined 4 tiers of service . Tier 1 services are identified as essential and critical services. They are critical to public safety and order; enabling support services workings for frontline essential services: •Frontline health care •Health protection services •Teachers •Emergency services workers including police, fire fighters, ambulance and SES •Technological support for essential services (ICT, information and data management •Waste collection •Capital Linen (contracted to ACT health) •Corrections (including Community Corrections, youth Justice, Child protection workers) •Public safety workers essential to the justice system including Courts and Tribunal, legal aid, DPP, certain registry personnel, FMC and Sheriffs •Access Canberra •Victims support and Public Advocate •Emergency maintenance •Legal, policy and drafting services
Emergency / Disaster Management	Criteria based on NERAG criteria and contextualised to represent losses from an emergency eg bushfire or flood.
Protective Security	The consequences of threats, risks and vulnerabilities that affect the protection of people, information and assets are inherent to many of the consequence categories listed and may be considered as part of a risk assessment.

ATTACHMENT B – GUIDELINES FOR DEVELOPING A RISK MANAGEMENT PLAN FOR A PROGRAM OR PROJECT

Projects and Programs undertaken by the CFC are required to establish a Risk Management Plan (RMP) and Risk Register at the inception of each program or project.

There is no standard or generally accepted format for an RMP. The way in which the RMP is developed will depend largely on the size, scope and complexity of the program or project that it relates to. Smaller projects may include the RMP as part of the overall project plan with a separate risk register. Alternatively, larger and more complex work programs will ordinarily require a separate standalone RMP.

Components of a Risk Management Plan (RMP)

An RMP should seek to minimise exposure to significant risks through the identification, assessment and management of individual risks, as well as to enhance the ability to capitalise on opportunities through minimising risks and improving overall performance indicators of the Program or Project.

A good RMP should clearly incorporate the following components and subsequent elements into its overall structure:

1. **Introduction**
    a) RMP Purpose
        - To manage the actions of identifying, assessing and treating risks to the program / project objectives and the resulting deliverables.
        - To create, maintain and report upon the risk register.
    b) Identify the intended audience
2. **Objectives and scope of the risk management plan**
    a) General – risk is to be managed:
        - In accordance with the AS ISO 31000:2018 Risk Management Principles and Guidelines
        - The CFC Risk Management Framework and Policy
    b) Risk Management objectives
        - Broadly to identify and appropriately treat and manage risks affecting program / project objectives. (This is the context for the risk assessment)
    c) The risk criteria
        - The criteria to be used in the risk assessment – the ACT Government risk management matrix tailored to the constraints of the program and/or project. Refer to Attachment B – Appendix one below for a template.
3. **The risk management organisation and reporting structures**
    a) Roles and responsibilities
        - Identify all roles that have responsibilities that include risk management and outline those responsibilities

b) Resources

- Identify and outline the resources available for risk management, budget and control.

c) Structure

- Including relationships with stakeholders outside the program / project boundary

4. Risk assessment

a) Communication and consultation

b) Risk identification

c) Risk analysis

d) Risk evaluation

e) Risk treatment

5. Risk management monitoring and review

a) Arrangements for risk monitoring including the authority for acceptance and continued tolerance of risks

b) Risk Reviews

- Frequency and arrangements for periodic reviews, reviews relating to milestones and other reviews.

c) Risk Reporting

- Nature, frequency and recipients of the risk management reports
- Co-ordination with other related projects or programs that will affect the successful delivery of each.

6. Risk register

a) The risk register is ordinarily a separate document. The risk register is a tool used to record the results of the risk assessment. The risk register should be a living document that is reviewed and updated regularly.

b) The most current version of the risk register can be attached to the RMP

Attachment B – Appendix - Part 1 - CFC Program / Project Risk

Likelihood	Frequency			Consequence					
				Matrix	Insignificant	Minor	Moderate	Major	Catastrophic
					1	2	3	4	5
	Almost Certain	Occurs on most occurrences of the activity	Expected to happen this time	**5**	**Medium**	**High**	**High**	**Extreme**	**Extreme**
	Likely	Occurs on some occurrences of the activity	Expected to occur on one of the next few occasions	**4**	**Medium**	**Medium**	**High**	**High**	**Extreme**
	Possible	Infrequently occurs here	Could occur at some time in the future. Would not be surprised if it occurred.	**3**	**Low**	**Medium**	**Medium**	**High**	**Extreme**
	Unlikely	Has never occurred here	Might occur but unlikely. Would be surprised if it occurred.	**2**	**Low**	**Medium**	**Medium**	**High**	**High**
	Rare	Has never occurred here, but may have/has occurred somewhere	Might occur, but only in exceptional circumstances. Would be very surprised if occurred.	**1**	**Low**	**Low**	**Medium**	**Medium**	**High**

	Suggested Timing of Treatment	Authority for the continued tolerance of risk		
		Program	Project	Authority for the tolerance of risk
Extreme	Short term – normally within one month Detailed action plan required			CEO
High	Medium term – normally within three months			Senior Management team
Medium	Normally within 1 year Specify management responsibility			Managers
Low	Ongoing control as part of a management system. Manage by routine procedures			Staff

Control Effectiveness	Guide
Adequate	Controls are well designed and operating effectively in treating the root cause of the risk. Additional controls exist to appropriately manage consequences. Controls are largely preventative, and management believes that they are effective and reliable at all times. Nothing further to be done except review and monitor existing controls.
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, controls are largely reactive. There are opportunities to improve the design/implementation of some controls to improve operational effectiveness.
Inadequate	Significant control deficiencies 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 of the effectiveness of the controls due to poor control design and/or very limited operational effectiveness.

		Consequence of risk in the most normal form				
Category of Risk	**Contextual definition**	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Business Operations	Achievement of strategic and operational business objectives	Minor errors in systems or processes requiring corrective action and/or minor delay without impact on overall schedule and/or insignificant impact on business outcomes and strategic objectives.	Services (including those of providers) do not fully meet needs and/or minor impact on business outcomes and strategic objectives and/or subsidiary services experience minor disruptions.	One or more key accountability requirements not met and /or inconvenient but not client welfare threatening and/or moderate impact on business outcomes and strategic objectives and/or a number of objectives not met, minor or subsidiary services impaired.	Significant impact on business and / or strategic objectives and/or strategies not consistent with Government's agenda and/or trends show service is degraded and/or key service delivery impaired.	Strategic business outcomes/ processes fail, control infrastructure failure, critical business objectives not met.
Service Delivery	Delivery of functions of the business/branch/ entity depending on their classification as essential/critical or not	No loss of an essential/critical service and/or loss of, or interruption to, non critical/non-core services up to 3 days.	Loss of an essential/critical service for less than 4 hours and/or loss of, or interruption to, non critical/non-core services for 3 - 5 days.	Loss of one or more essential/critical services for more than 4 hours and up to 3 days, and/or loss of, or disruption to, non critical/non-core services for up to 10 days.	Loss of one or more essential/critical services for more than 3 days and up to 4 or more weeks, and/or loss of part of an essential service that is high risk (life based) and/or disruption to non-critical services over subsequent weeks.	Loss of one or more essential/critical services for more than 4 weeks that continues for months and/or loss of an essential service that is high risk (life based) and/or disruption to non-critical services over subsequent months.
Compliance/Regulation	Non compliance with legislation, regulation, policy or procedure (including conflicts of interest), and the associated consequences to operations	Non-compliance with policies, procedures & guidelines and standard operating procedures which are not legislated or regulated.	Numerous instances of non-compliance with work policy and standard operating procedures which are not legislated or regulated.	Non-compliance with work policy and standard operating procedures which are regulated or legislated.	Restriction of business operations by regulator due to non-compliance with relevant guidelines and / or significant non-compliance with policy and procedures which threaten business delivery.	Operations shut down by regulator for failing to comply with relevant guidelines / legislation and /or significant non-compliance with internal procedures which could result in failure to provide business outcomes and service delivery.
Cultural & Heritage	Damage or adverse outcomes to items or places of cultural or heritage value	Consists of, but is not limited to, repairable damage or no impact to the heritage place or object and/or Unauthorised conduct to the heritage place or object, including Aboriginal places and object. The conduct has no or repairable impact.	Consists of, but is not limited to, repairable damage to the heritage places or object and/or Unauthorised conduct that diminishes the heritage significance of the place or object, including Aboriginal places and objects. The conduct has minor repairable adverse heritage impact.	Consists of, but not limited to, repairable or irreparable damage to the heritage place or object and/or Unauthorised conduct that diminishes the heritage significance of the place or object, including Aboriginal places and objects. The conduct may or may not have an acceptable heritage impact.	Consists of, but not limited to, significant, or irreparable damage, or total loss of the heritage place or object and /or Unauthorised conduct, including negligent conduct, that diminishes the heritage significance of the place or object, including Aboriginal places and objects. The conduct has an unacceptable heritage impact.	Consists of, but not limited to, permanent or irreparable damage, or total loss of the heritage place or object and/or Unauthorised conduct, including reckless conduct, that diminishes the heritage significance of the place or object, including Aboriginal places and objects. The conduct has an unacceptable heritage impact.
Financial	Financial losses from the project or entity represented as either a percentage of the project/entity budget or a dollar amount, which ever is the greater	1% of Project / Entity Budget or <$5K	2.5% of Project / Entity Budget or <$50K	> 5% of Project / Entity Budget or <$500K	> 10% of Project / Entity Budget or <$5M	>25% of Project / Entity Budget or >$5M
Information & Records Management	Access to and security of information and records that enable the conduct of business and provision of services	A product or service which services up to 10% of the workforce or impacts a small number of the community in a minor way and/or System breach to business administration system with no personal or classified information stored.	A product or service which services 10 - 30% of the workforce or impacts a small number of the community in a moderate way and/or System breach to business administration system with some identifiable information but non-client threatening (data access known).	A product or service which services 30-70% of the workforce or impacts a moderate number of the community in a moderate way and/or System breach to business administration system with some identifiable information but non-client threatening (data access unknown).	A product or service which services greater than 70% of the workforce or impacts a small to moderate number of the community in a major way and/or Systems breach to business administration system with identifiable/classified information stored but non-client welfare threatening.	A product or service which services 100% of the workforce or impacts a moderate or substantial number of the community in a major way and/or total loss of confidence in data/record integrity and/or Systems breach to Government or business critical systems with client and/or business welfare threatened.
Natural Environment	Adverse outcomes for the natural environment	Environmental harm to an ecosystem and species is limited to a localised area with rapid recovery without effort.	Minimal environmental harm to an ecosystem and species recognised at the local or regional level and/or Localised but minor instances of environmental harm that can be reversed with minimal efforts.	Moderate environmental harm to an ecosystem and species recognised at the state level and/or Semi-permanent loss of environmental value and risk of continuing environmental harm.	Major environmental harm to an ecosystem and species recognised at the national level and/or Loss or impairment to an ecosystem or species recognised at the state or regional level and/or Difficulty recovering from environment damage and stemming ongoing environmental harm.	Severe Damage and/or significant loss and/ or impairment and/or Permanent destruction of an ecosystem or species recognised at the local, regional, state or national level and/or Permanent and widespread loss of environmental value and progressive irrecoverable environmental harm.
People Injuries (physical & psychological)	Direct physical and psychological injuries to people (staff, contractors, customers) arising from the risk occurring. The impact to people arising from Natural Disaster related events is covered under the Emergency / Disaster Management categories	No injury or treatment required.	Injury which: •requires treatment (not hospitalisation); and/or •impacts capacity to work for a period of one week or less; and/or multiple people sustain injury/ies not requiring treatment.	Injury which: •requires hospitalisation; and/or •impacts on capacity to work for a period of greater than one week; and/or multiple people sustain injury/ies which: •require treatment •impact their capacity to work for a period of one week or less.	Single injury which: •is life-threatening (including loss of limbs); and /or •results in permanent disability; and /or •results in permanent (partial or total) impact on capacity to work; and /or multiple people sustain injury/ies which: •require hospitalisation •impact their capacity to work for greater than one week.	Death and/or multiple injury/ies which result in: •permanent impact on capacity to work; and/or •permanent disability.
Reputation & Image	Observable measures of how the risk may impact the reputation or image of the ACT Government	Internal review and/or minor dissatisfaction across a small number of demographic groups or stakeholders.	Scrutiny required by internal committees or internal audit to prevent escalation and/or moderate dissatisfaction across a small number demographic groups or several stakeholders.	Local media scrutiny (1 week) and/or scrutiny required by external committees or ACT Auditor General's Office, or inquest, etc and/or dissatisfaction across a few demographic groups or multiple stakeholders.	Intense public, political and national media scrutiny (1 week) and/or Minister / Chief Minister involvement and/or dissatisfaction across a large range of demographic groups and stakeholders.	Adverse finding from Assembly Inquiry or Commission of Inquiry or sustained adverse international media and/or loss of public confidence in Government or Public Service forcing changes to the machinery of Government.
Emergency / Disaster Management (social impact)	Measures of the social impact to the ACT arising from emergencies (eg bushfire, flood, storm damage etc)	The community's social connectedness is disrupted, such that the reprioritisation and / or reallocation of existing resources is required to return the community to functioning effectively, with no permanent dispersal.	The community's social connectedness is disrupted, such that community requires some external resources to return the community to functioning effectively, with no permanent dispersal.	The community's social connectedness is disrupted, such that community requires significant external resources to return the community to functioning effectively, with some permanent dispersal.	The community's social connectedness is significantly disrupted, such that extraordinary external resources are required to return the community to functioning effectively, with significant permanent dispersal.	The community's social connectedness is irreparably disrupted, such that the community ceases to function effectively, breaks down and disperses in its entirety.
Emergency / Disaster Management (community / people impact)	Outcomes on the community or people of the ACT arising from emergencies (eg bushfire, flood, storm damage etc).	Minor injuries to 10 or less people.	Less than 4 serious injuries, or more than 10 minor injuries directly from the emergency.	Less than 4 deaths or critical injuries with long-term or permanent incapacitation, directly from the emergency, or more than 4 serious injuries.	4 – 40 deaths or critical injuries with long-term or permanent incapacitation, directly from the emergency, or more than 40 serious injuries.	More than 40 deaths or critical injuries with long-term or permanent incapacitation, directly from the emergency.