CULTURAL FACILITIES CORPORATION
Risk Management Framework and Policy

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 PROPERTIES

Schedule of Amendments

New features (insertions)	
	Date
Enhancements (changes)	
	Date
Deletions	
	Date

Amendment History

Version No.	**Issue Date**	**Author**
Version 1.0	November 2021	Ian Tidy

Details

Prepared for	All Cultural Facilities Corporation Staff
Document Owner	Chief Finance Officer/Senior Executive Responsible for Business Integrity Risk
File Name	Cultural Facilities Corporation Risk Management Framework and Policy
Document location	G:\CFC\Staff\Documents\CFC
Status	Final
***Freedom of Information Act 2016* compliant**	Document linked to the ACT Open Access Information website? No ☐ (the document is not appropriate for public viewing) Yes ☒ (the document is appropriate for public viewing)

Contents

INTRODUCTION

Purpose

Effective risk management is regarded as essential for the development and delivery of quality services across the ACT Government, its Ministers and the ACT community. It helps in determining an appropriate control environment and balance of strategies to address risk in order to ensure efficient and effective utilisation of resources.

The Cultural Facilities Corporation (CFC) is committed to ensuring that all business and operational processes are underpinned by an effective risk management process.

The CFC's Risk Management Framework provides the foundation and organisational arrangement for how risk is managed across the agency. This Framework will assist the CFC in being well-placed to achieve its objectives and ensure risk management processes are embedded consistently across the CFC. The purpose of this Framework is to integrate the process for managing risk into the CFC's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

The CFC Board has overarching responsibility for the CFC's risk management. Under Section 77 of the *Financial Management Act 1996*, the Board is responsible for setting the CFC's policies and strategies for risk management, including through approval of this Framework and Policy. The Board has identified its specific roles and responsibilities for risk management through the Board Charter, including the risk management responsibilities of the Board's Audit Committee.

The CFC Senior Management team 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.

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

- 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;
- anticipating future occurrences and 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 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.

Scope

The CFC's Risk Management Framework is consistent with the ACT Government Risk Management Policy 2019 and the AS ISO 31000:2018 Risk Management – Principles and Guidelines standard. This document provides:

- a risk management policy statement clearly stating the CFC's commitment to risk management;
- an outline of the principles of risk management which are to be applied;
- details of the CFC's risk management framework;
- an overview of the roles and responsibilities for managing risk (governance arrangements); and
- details of internal and external communication and reporting mechanisms.

Application

Application of the Framework and Policy should be applied across all aspects of the CFC's business and operations at all levels.

RISK MANAGEMENT POLICY STATEMENT

Risk management in the CFC is based on the Australian Risk Management Standard (AS ISO 31000:2018) ('The Standard').

The approach to risk management in the CFC shall support the ACT Government's commitment to 'managing risk to meet its fiscal, social and environmental responsibilities'.

All staff are to demonstrate their commitment to robust risk management practices by adopting and implementing risk management in line with 'The Standard', the CFC Risk Management Framework and the CFC Risk Management Plan.

Risk is inherent in all CFC's functions and elimination of all risk is not practical or appropriate. Therefore, risk management principles are to be integrated in all aspects of CFC's work. A strategic and systematic approach to risk management, aligned with organisational objectives and strategies, will enable sound judgments and decision-making, cost effective use of resources and maximise potential opportunities while minimising adverse consequences.

CFC planning processes, including strategic and business planning, together with policy development and project management will incorporate risk management. Risks and any necessary 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 delivery and 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 on risk management and, as appropriate, be provided with opportunities to contribute to risk identification, assessment and management processes.

Risk management in the CFC will be monitored by the CFC Senior Management team reporting to the CFC Audit Committee and the CFC Board.

WHAT IS RISK MANAGEMENT

Australian Standard AS ISO 31000:2018 Risk Management – Principles and Guidelines defines risk as the effect of uncertainty (either positive or negative) on business objectives.

Risk management is the coordination of activities that direct and control the agency about risks. It is commonly accepted that risk management involves both the management of potentially adverse effects as well as the realisation of potential opportunities.

In performing our daily activities and responsibilities, risk management can be described as the collection of deliberate actions and activities that we carry out at all levels to identify, understand and manage risks to the achievement of our objectives.

A risk is often specified in terms of an event or circumstance and the consequences that may flow from it. Risk is measured in terms of a combination of the consequences of an event and the likelihood of it occurring.

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 giving advice 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 Policy 2019.

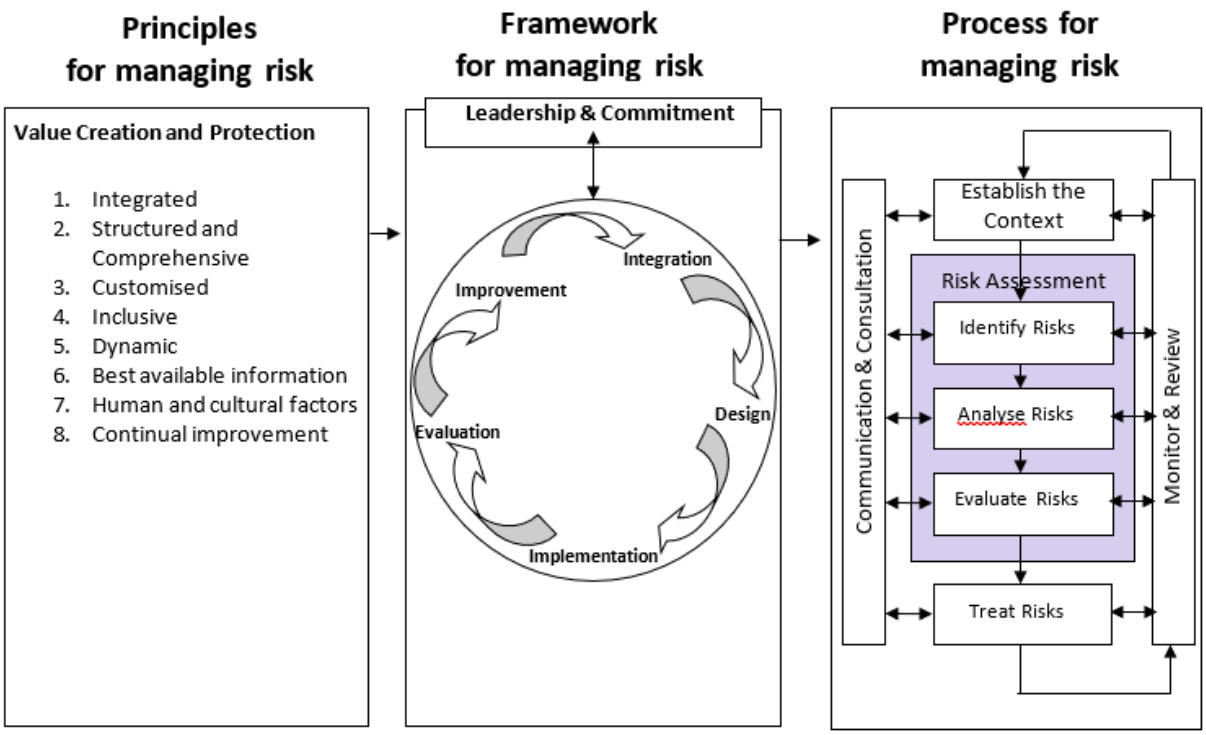
The Risk Matrix, Risk Registers and Risk Treatment Action Plans used by CFC are based on those developed by ACTIA. These documents have been developed to be consistent with the AS ISO 31000:2018 standard.

AS ISO 31000:2018 is separated into three core areas:

- principles
- framework
- process (refer to *CFC 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.

Diagram 1: Principles, framework and process



RISK MANAGEMENT PRINCIPLES

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.

The principles of risk management when embedded within the CFC enable the CFC 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.

CFC RISK MANAGEMENT PLAN

In addition to the Risk Management Framework and Policy, the ***CFC Risk Management Plan*** consists of components and tools intended to assist the CFC with undertaking effective risk identification and analysis processes.

GOVERNANCE ARRANGEMENTS

Risk governance includes mechanisms that ensure accountability and authority for the management of risk (identifying, assessing, treating and monitoring and reviewing risks) implementation, maintenance and continuous improvement of the CFC's risk management framework, and providing risk management assurance.

Roles and accountabilities within the CFC are outlined as follows:

CFC Board

- Set the CFC's policies and strategies for risk management, including through approval of the ***CFC's Risk Management Framework and Policy***; ***Risk Management Plan***; ***Strategic Risk Management Register***; ***Fraud and Corruption Prevention Plan and Policy***; and ***Fraud Risk Register*** and
- Ensure that risks facing the CFC have been identified and assessed and that the risks are being properly managed.

CFC Audit Committee

- Review whether management has in place a current and comprehensive risk management framework, including through the ***CFC's Strategic Risk Management Framework and Policy, Strategic Risk Management Register, Fraud and Corruption Prevention Plan and Policy, and Fraud Risk Register***; and other associated policies, plans and procedures for effective identification and management of the CFC's :
    - financial and business risks, including by monitoring insurance arrangements; and
    - business continuity planning arrangements, including periodic testing of disaster recovery plans; and
- Review the ***CFC's Fraud and Corruption Prevention Plan and Policy and CFC's Fraud Risk Register*** to ensure the CFC has appropriate processes and systems in place to capture and effectively investigate fraud related information.

CFC Senior Management team

- Review and update the ***CFC Risk Management Framework and Policy***;
- Review and update the ***CFC Risk Management Plan***;
- Review and update the ***CFC Strategic Management Register, Fraud and Corruption Prevention policy and plan,*** and the ***CFC Fraud Risk Register***;
- Oversee the CFC's Risk Profile, including fraud and integrity risks;
- Establish parameters for risk exposure and tolerance levels; and
- Review yearly risk updates incorporating risk management, business continuity and fraud prevention activity.

Business Unit Directors

- Incorporate risk management principles into all aspects of business activities;
- Ensure staff understand their risk management responsibilities;
- Review and update their relevant risk profiles, registers and plans;
- Ensure that business plans include a discussion of key issues and major risks;
- Ensure project plans incorporate risk management processes that are scaled appropriately to align with magnitude and complexity of the project;

- Identify, analyse and evaluate risks and treat risks in a manner commensurate with the level of risk exposure;
- Encourage innovation and take advantage of emerging opportunities to optimise outcomes in a cost-effective manner and consistent with risk management principles;
- Monitor compliance with risk management policies, this framework and risk treatment plans;
- Align organisational and risk management objectives, strategies and performance indicators; and
- Advise the CEO and CFO of relevant risk management matters.

Managers and Supervisors

- Foster a risk aware culture;
- Create an environment where managing risk forms the basis of all activities;
- Regularly review the adequacy of controls to ensure that they are operating effectively and are appropriate for achieving organisational goals and objectives; and
- Create an environment where staff are encouraged to develop skills, actively participate in processes and identify and communicate potential risks.

Staff and Contractors

- Develop an understanding of the organisational policy, framework and procedures, and their application;
- Comply with all legislative, regulatory and organisational policies;
- Adopt sound risk management practices by identifying, analysing, evaluating and treating risks that might impact on their objectives;
- Maintain an awareness of risks that relate to their area of responsibility and encouraging a risk-aware culture in their work area;
- Monitor, communicate, and report risks to provide early warning systems of risk occurrences and consequences;
- Actively support and contribute to risk management initiatives; and
- Look for opportunities which will improve operational efficiencies and optimise outcomes.

Program / Project Manager

- Develop a risk management plan for the program/project that describes how risk will be managed throughout the lifecycle of the program / project:
    - the risk management plan should include how risk is to be managed and reported for any related projects that form part of the program of work;
- Create an operating environment for the lifecycle of the program / project where managing risk is embedded into the management and reporting requirements for the program at all stages of the program / project lifecycle;
- Adopt sound risk management practices within the program by identifying, analysing, evaluating and treating risks that might impact on the objectives of the program / project;
- Comply with all legislative, regulatory and organisational policies;
- Actively support and contribute to risk management initiatives; and
- Look for opportunities which will improve operational efficiencies and optimise the program / project delivery outcomes.

Senior Executive Responsible for Business Integrity Risk (SERBIR)

- Coordinate annual reporting on fraud prevention and control activity;
- Arrange investigations of allegations of suspected fraud and misconduct;
- Collate and maintain the Risk Register;
- Maintain the ***CFC Risk Management Framework and Policy***, and the ***CFC Risk Management Plan***;
- Collate information from the Risk Registers; and
- Report to the Audit Committee and Board.

MANAGING RISK WITHIN THE CFC

The identification and management of risk is best undertaken by those closest to the risk.

The ACT Insurance Authority (ACTIA) has overarching policy responsibility for risk management in the ACT Public Service and has developed the following list of potential categories of risk for use in the development of risk registers and plans. Consideration should be given to all the following when developing and reviewing risk management plans:

- Assets
- Business processes and systems
- Commercial
- Compliance / regulation
- Contractual
- Cultural Heritage
- Environment
- Financial
- Fraud
- General Management Activities
- Operational
- People (there are multiple types of People risk subcategories)
- Products and Services
- Project
- Records Management
- Reputation and Image
- Technology
- Security
- Stakeholder Management
- Strategic
- Technology
- Other

The following table reflects the process CFC follows to manage risk:

Process	Description
Tasks	• Output from risk assessments to be held in Risk Registers. • Nominated Risk Owners to be identified. • Risk Treatment Action Plans to be developed and implemented to ensure that plan objectives and budgets are met. • Risk treatment actions to be allocated to nominated task owners and tracked and monitored for completion and measurable (or observable) effectiveness. • Regular reviews identifying new or emerging risks that might affect the achievement of strategic and business plan objectives and budgets.
Timeframes	• Conduct reviews of existing risks at a minimum of yearly including the progress with Risk Treatment Action Plans. • Programs/Projects are to conduct reviews of existing risks on a regular basis in accordance with normal program management requirements.
Reporting	• Report identified risks to the Senior Management Team • Program/Project Managers will report identified program risks and any identified risk owner to the business unit Director.

RISK PERFORMANCE MEASURES

CFC measures its risk management performance by monitoring on a regular basis, the implementation of treatment/control strategies. Reporting occurs against the following performance measurement framework:

Risk Performance Measures

Key Objective	Performance Indicators	Measured by
1. Increased risk sensitivity and awareness	• Increased or enhanced staff knowledge and awareness of risk management concepts and principles	• Attendance at risk related training • Risk management integrated into business plans • Risk management integrated into performance agreements • Local discussion of risk
2. Improved risk identification and management	• Business risks, including fraud and integrity risks, are identified and tracked (such as through risk registers) across the CFC • Business areas identify risk owners and budget	• Business area Risk Registers and Treatment Plans updated annually • SERBIR reports to CEO on the integration of fraud prevention arrangements • SERBIR reports to the Audit Committee level of local discussion of risk

Key Objective	Performance Indicators	Measured by
	for, and implement risk treatment/control strategies	
3. Integration of risk assessment into strategic, operation and reporting activities	• Business plans include a discussion of key issues and major risks • Business Continuity Plan developed and tested	• Risk management integrated into business plans • SERBIR reports to CEO on Strategic Risks and Business Continuity Plan testing and currency • SERBIR reports to Audit Committee and Board on Strategic Risks and Business Continuity Plan testing and currency
4. Increased awareness of the Code of Conduct, values, ethics and accountability	• Investigations initiated promptly and where required, management or legal actions are taken • Investigations conducted by appropriately qualified individuals	• Allegations of fraud or misconduct are assessed on a preliminary basis within one month with preliminary assessments completed within three months wherever possible • Investigations are conducted in accordance with the ACTPS Fraud Control Guidelines • Disciplinary, civil or criminal actions taken as required

ASSURANCE AND CONTINUOUS IMPROVEMENT

Reporting Compliance with the ACT Government Risk Management Framework

The CFC will report its risk management and internal audit policies and practices in annual reports. The CFC is required to confirm that it understands, manages and controls key risk exposures and that the Audit Committee verifies agency arrangements.

Monitoring and Reporting of Risk Management

Regular monitoring and review must be a planned part of the risk management process. Its purpose serves to ensure that:

- controls are effective and efficient in design and operation;
- lessons are learned from events, changes, trends, successes and failures;
- changes in the external and internal context, including the risk criteria are detected and revised;
- emerging risks are identified;
- risk performance against indicators;
- adequacy of the risk management framework, policy and plan and whether they remain relevant and appropriate given the organisations' external and internal context;
- there is compliance with the risk management policy; and
- there is effectiveness of the risk management framework.

Where a risk is identified, or changed, and needs to be immediately reviewed and occurs between nominated review dates, the risk should be immediately addressed and reported to the appropriate manager.

The table below provides detailed information of the tasks, forming part of the monitoring and review process.

Monitoring and Review tasks and timelines

Process	Description

Tasks	The ACT Government requires the following risk management reporting regime to be followed:
	
	Risk Governance – consistent with the requirements of the Chief Minister's Annual Reporting Directions, the CFC is required to report the following:
	
	• membership of the Audit Committee, with details of:
	  – the number of meetings held by the committee; and
	  – the number of meetings attended by committee members
	• internal audit arrangements, including Audit Committee charter and operations, and links with risk review processes;
	• process for developing the CFC's risk management plan;
	• approach adopted to identify areas of significant operational or financial risk at Business Unit level;
	• arrangements in place to manage and monitor those risks; and
	• processes for identifying and responding to emerging risks.
	
	Risk Profile – all risks rated 'Extreme' or 'High' or where risk controls are less than 'Adequate' will be reported to the CFC Board. In these cases a Risk Treatment Action Plan for those risks should also be submitted.
	
	Senior Managers will ensure that Risk Registers and Treatment Action Plans are up-to-date.
	
	Performance measures and targets are to be specified for risk management and for achieving compliance with the Framework and Policy.

FRAMEWORK COMPLIANCE AUDITS

Regular internal audits of risk management are to be completed to ensure effective management of risk and compliance with the Framework by all business areas. Audit reviews by independent external parties may be undertaken if deemed appropriate.

The ACT Auditor-General is responsible for undertaking independent audits of management performance and the financial statements of CFC. This may include periodic reviewing and reporting on the level of compliance of CFC with governance frameworks including risk management.

REVIEW

Continuous improvement is strategically integrated with the CFC's corporate objectives to ensure that the CFC continues to evolve towards best practice.

The Senior Management team will review the Framework every two years and will ensure that the Framework and associated business processes continue to meet local needs as risk management matures and improves.