Risk Management Procedures

Associated Policy

These procedures should be read in conjunction with the CIT Risk Management Policy.

Introduction

Risk management is an integral part of good corporate governance. Adopting good risk management practices that are embedded within organisational processes and linked to strategic objectives ensures appropriate measures are in place to identify opportunities and minimise the effects of risk.

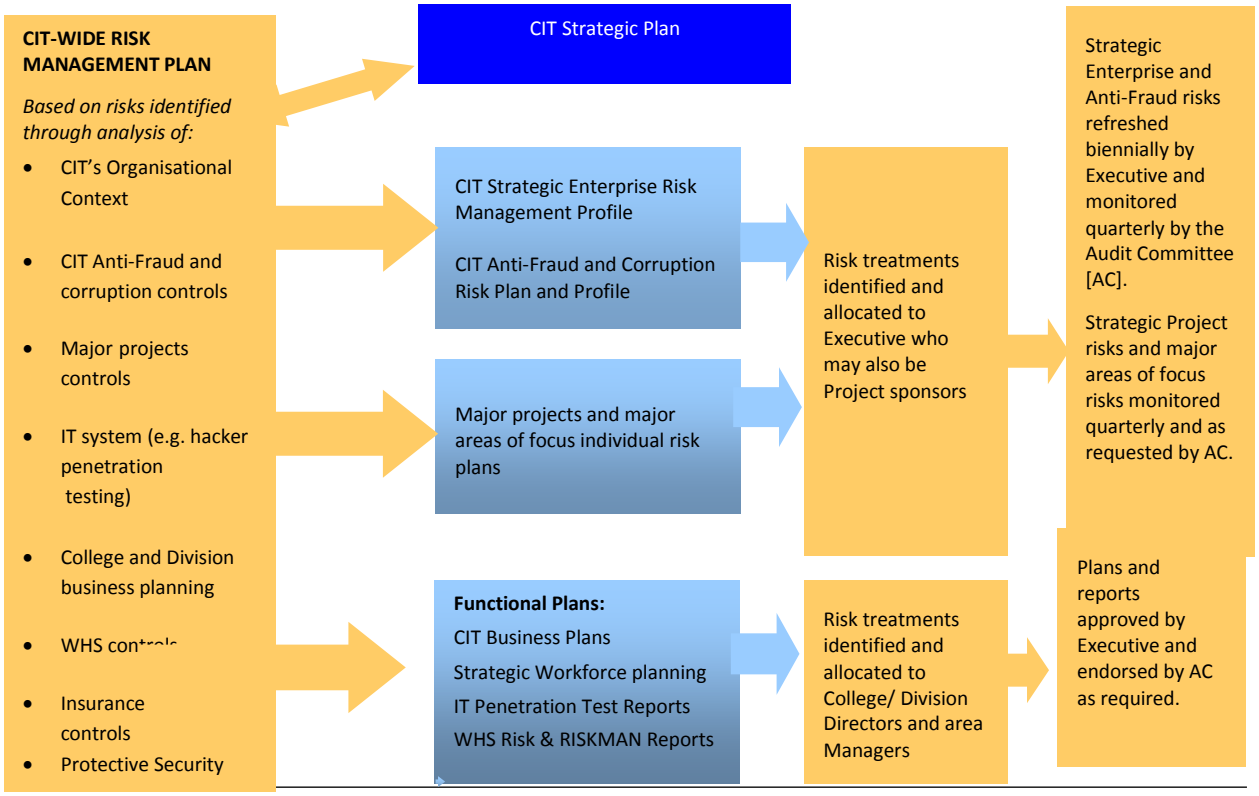
There is an element of uncertainty in everything we do, any changes that are undertaken or any improvements implemented. Risks are managed by putting in place controls to mitigate (reduce) the likelihood of the risk event happening, and the impact on CIT if the risk event were to happen. Hence, risk management is central to CIT's control structures and therefore, its corporate governance.

CIT has adopted an organisational-wide approach, integrating risk management strategies with CIT's business processes.

CIT's risk management framework

CIT's risk management framework is set out in **Diagram 1**. The following framework has been developed to demonstrate the interdependency of risks across the Institute and how it is an integrated part of CIT's Planning Process. This framework provides a defensible strategic focus.

Diagram 1



When to conduct a risk assessment

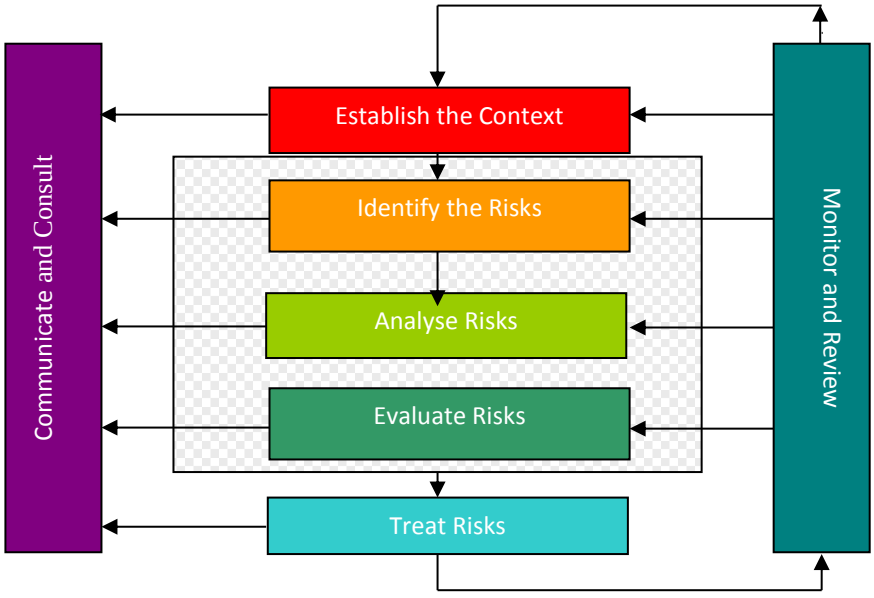
Risk assessments are conducted at three levels in CIT:

- A CIT-wide risk assessment in relation to CIT's strategic enterprise risk and anti-fraud and corruption risks, is conducted on a biennial basis, with quarterly and six monthly reviews, respectively
- CIT-wide strategic project risks should be assessed throughout any project as required
- College/ Division business plan risks and functional plan risks with six monthly reviews e.g. WHS risk assessments should be conducted annually.

Responsibilities for Risk Management

CIT Board	Receives assurance from the CEO that CIT has an effective risk management system that is reviewed by Executive and monitored by the Audit Committee at regular intervals. The Risk appetite is established by the CIT Board.
Chief Executive Officer	Establishes the process for risk management across CIT and advises the CIT Board Chair.
Audit Committee	Oversees quarterly review of the Strategic Enterprise Risk Management Profile, and practices and reports to the CEO and CIT Board as appropriate, on any issues arising.
Audit, Risk and Corporate Governance Team	Facilitates the Executive identification of both current and emerging strategic risks, including developing mitigation strategies, risk ratings, timelines, and ownership; and co-ordinates the development of the CIT Strategic Enterprise Risk Management Profile; and monitors the updates of quarterly (Enterprise Risk) and six monthly reports (Anti-fraud).
Directors, and Senior Managers	Accountable with their staff for the identification of risk and implementation of sound risk management processes within their areas of responsibility; and that specific business risks are embedded within their CIT Business Plans.
Staff and Contractors	Understand and apply risk management policies and practices in working towards corporate objectives.

Diagram 2 - *Steps undertaken for risk management*



Procedures

1. Establishing the organisational context

A consultative team approach is useful to help define the context, to ensure risks are identified effectively, for bringing different areas of expertise together in analysing risks, for ensuring different views are considered in evaluating risks, and for appropriate change management during risk treatment. Involvement also allows the 'ownership' of risk by managers and the engagement of stakeholders.

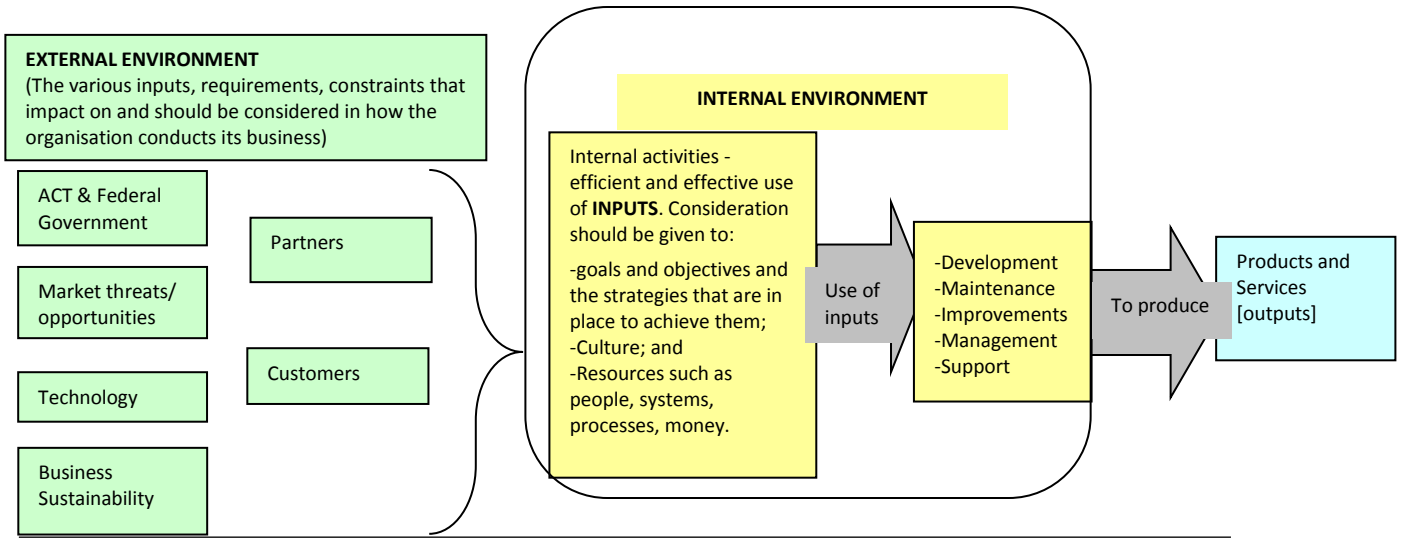
External Context

- understanding the broader CIT environment: e.g. government requirements, community expectation, political pressures, customer expectations, technology, impact of other agencies such as Shared Services etc.
- developing awareness of the full range of factors which form the environment
- understanding the nature of CIT's competition
- understanding what differentiates CIT from its competition
- identifying key stakeholders, clients and their objectives/perceptions and how to communicate with them
- identifying the major issues influencing risks in relation to the risks.

Internal Context

- understanding the internal environment of CIT e.g. strengths, weaknesses, opportunities, threats, and key business drivers etc.
- identifying the key objectives and outcomes including the timeframe within which you will want to consider the impact of a risk event if it were to occur
- understanding the culture
- identifying the internal stakeholders
- identifying the key decision makers
- assessing the capabilities in terms of resources such as people, systems, processes, capital.

Diagram 2: Graphic description of the process for the internal and external environment



2. Identify the risks

Unidentified risks can pose a major threat to both a project and CIT. The risk identification process should:

- examine all sources of risk, both internal and external
- align with CIT's Strategic Plan and College/ Division Business Plans
- take account of the perspectives of all internal and external stakeholders
- use good quality information that is relevant, comprehensive, accurate and timely.

Components of Risk include:

- a **source** of risk or hazard – the thing which has the potential to harm or assist e.g. a dangerous chemical, competitors, government
- an **event or incident** – something that occurs that has an impact e.g. a leak, competitor expands into or leaves your market area, new or revised regulations, or some measure or observation reaching a particular trigger level
- a **consequence**, outcome or impact on a range of stakeholders and assets e.g. environmental damage, loss or increase of market/profits, regulations increase or decrease competitiveness
- a **cause** (what and why) for the presence of the hazard or the event occurring e.g. design, human intervention, funding, prediction or failure to predict competitor activity, failure to or expansion of market presence
- **controls** and their level of effectiveness e.g. detection systems, clean up systems, policies, security, training, market research and surveillance of the market
- **when** could the risk occur and **where** could it occur.

Further information on risk identification is at Appendix A.

3. Analyse the risks

Risk analysis involves consideration of the sources of risk, their positive and negative consequences and the likelihood that those consequences may occur. Risk is analysed by combining consequences and their likelihood to establish the level of risk.

- The **likelihood** of the risk occurring; and
- The **consequences** or **degree of impact** on CIT if it did occur.

The assessments of likelihood, consequence and the overall risk should be made using the ACTIA – ACT Government Risk Matrix at **Appendix B.**

Once a risk has been identified a current risk rating, based on likelihood of it happening and the consequences, should be determined. Current ratings take into account existing controls only and **not** proposed treatments.

Example: Ineffective controls surrounding corporate credit cards resulting in inappropriate use of CIT funds and/or fraudulent activity (**effect or impact).**

Likelihood Rating: Possible	Consequence: Moderate
Likelihood factors: ▪ New staff not aware of policies and procedures ▪ Increased credit card expenditure ▪ Training has not been provided in a timely manner ▪ Removal of petty cash floats **Current controls to prevent the event** ▪ Policies and procedures in relation to procurement ▪ Independent review of credit card statements	**Consequences:** ▪ Misuse of CIT funds ▪ Potential threat to program budgets, depending on magnitude ▪ Ramifications of fraudulent behaviour ▪ Criticism from community in relation to misuse of public funds **Current controls to reduce the impact if the event occurs:** ▪ Policies and procedures in relation to procurement

Risk Rating: Possible and Moderate is a Medium risk rating: see Appendix B

4. Evaluate risks

After determining the current risk rating, a decision on whether action/treatments to reduce the level of risk to an acceptable level are needed to identify management priorities.

Knowledge of the business, past and present, and awareness of emerging issues are fundamental when making a decision. Implementing treatments to reduce a risk rating generally requires resources (money and/or staff). Consideration must therefore be given to the cost and benefits to CIT in reducing a risk.

Within CIT, risk evaluation is undertaken by comparing the level of risk found during the analysis process against previously established risk criteria (see **Appendix C**).

The first consideration for CIT is to consider what level of risk tolerance is to be accepted, known as the Risk Appetite. For strategic business risk this is a CIT Board decision and then the level of tolerance should be mapped against the risk category and individual risks. Managers need to determine what level of risk they are prepared to accept within their College and Divisional business plans. This must be below the risk appetite set by the CIT Board.

5. Treat risks

Risk treatments (or controls) are designed to reduce the level of risk. Treatments either reduce:

- the likelihood of a risk occurring
- the consequence (or impact) of a risk event should it occur or
- both.

The following risk treatment options should be considered in this process:

- **Avoid the risk** by not proceeding with the policy, program, project or activity which would incur the risk.
- **Treat the level of risk** by reducing the probability of occurrence or the impact of occurrence. For example, the probability of occurrence might be reduced by such things as more research, increased controls, revised organisational arrangements, improved project management, increased monitoring, improved training or better planning. The impacts of occurrence might be reduced by such things as contingency planning, disaster recovery plans, effective contractual arrangements, stakeholder consultation and improved public diplomacy.

- **Transfer the risk** by shifting responsibility for the risk to another party. This might be done by contract, insurance, legislation or administrative processes. It is essential that where risk is transferred that principles of fairness and equity be observed so as not to disadvantage clients or others in a poor position to accept the risk. For CIT core activities, risk transfer may not be a viable option.
- **Accept and manage the risk** where the risk cannot be avoided, transferred or reduced, or where the cost of doing so cannot be justified.

In developing treatment options first consider the Risk Appetite, whether the type and levels of risks are acceptable or unacceptable. For low or negligible these should be managed by routine procedures. However, a risk rated at extreme, high or medium might be acceptable if:

- there is no treatment available because the risk is not within the control of the CIT
- the cost of treatment is excessive compared to the benefit of treatment or
- the opportunities presented by the risk outweigh the threats to such a degree that the risk is justified.

It is rare that a risk treatment program will completely eliminate a risk. It is important that the remaining risk is clearly identified and that there is a clear understanding as to why the risk was accepted.

The amalgamation of all the identified treatments becomes the Risk Management Profile. This profile documents:

- the risks
- current risk rating [prior to further treatment]
- the actions to be taken for further treatment
- who is responsible for the action
- dates by when action items will be completed
- revised risk rating [after treatment].

6. Monitor and review

Risks and the risk management context should be monitored on a regular basis, as well as the effectiveness of the risk management strategy and plan adopted, to reassess their relevance due to changing circumstances.

Programs and processes change, as can political, social and legal environments and goals of the organisation. By measuring and monitoring changes to the business environment, improved information can be obtained for identification and analysis.

Review of the CIT Enterprise Risk Management Profile and Anti-Fraud and Corruption Control Plan and Profile is undertaken on a biennial cycle to re-examine the accuracy of information and judgements made and ensure that the Plan remains relevant.

Project/ Program risk assessments should be undertaken whenever there are changes made to the project or new information received. Few risks ever remain static and the suitability and cost of the various treatment options could change over time.

College/ Division business plan risks and functional risk plans should be assessed on an annual basis or as circumstances change.

Monitoring and quarterly reporting of strategic enterprise risk action plans takes place via reports to the Executive Management Committee, the Audit Committee and the CIT Board. As part of the Audit

Committee's Charter it examines risk at the CIT-wide level, (enterprise) and monitors the implementation of identified and resourced risk treatments. It also monitors risks and risk treatments in relation to major projects.

7. Record the risk management process

Each stage of the risk management process should be recorded appropriately. The records of such processes are an important aspect of good corporate governance. Subject to legislative requirements, decisions and processes involving risk management should be documented to the extent appropriate to the circumstances. The CIT Risk Profile template is at **Appendix D.**

8. Glossary of Terms

Term	Definition
AS ISO 31000:2018 Risk Management Guidelines	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.
Audit Committee	The *Financial Management Act (FMA) 1996* states that an audit committee is appointed to oversee and advise Directorates on matters of accountability and internal control. This committee is a subset of the Responsible Body (or Board) which has been formulated to deal with issues of a specific nature.
Consequence	The impact a risk event will have on objectives if it occurs.
Controls	Agreed actions to be taken (eg. processes, policies, devices, practices) to modify the magnitude of risk.
Incident	An event that has the capacity to lead to loss of or a disruption to an organisation's operations processes and functions, which if not managed, can escalate to an emergency, crisis or disaster.
Inherent Risk	The level of risk that is assessed taking into account the effectiveness of current controls.
Key Performance Indicators (KPIs)	Measures the effectiveness of the implementation of the risk management framework.
Key Risk Indicators (KRIs)	A measure and metric that relates to a specific risk and demonstrates a change in the likelihood or consequence of the risk occurring.
Likelihood	Probability or chance of something occurring.
Public sector	Entities that are controlled by the *Public Sector Management Act 1994*.
Residual Risk	The level of risk which is present after taking into account further treatments and the effectiveness of the treatments.
Risk	'Effect of uncertainty on objectives.'[6]
Risk Appetite	'Amount and type of risk that an organisation is willing to pursue or retain.'[7]
Risk Appetite Statement	Qualitative statement on the amount of risk that an organisation is willing to accept. This will include type of risk, amount of risk and risk thresholds for risk acceptance.
Risk Assessment	'The overall process of risk identification, risk analysis and risk evaluation.'[8]
Risk Criteria	'Terms of reference against which the significance of a risk is evaluated.'[9]
Risk Management	'Coordinated activities to direct and control an organisation with regard to risk.'[10]

Term	Definition
Risk Management Framework	A 'set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.'[11] Its purpose is to embed risk management across all major practices and business processes including business and strategic planning, policy development, asset management, audit, business continuity, fraud control and project management.
Risk Management Plan	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	Used to analyse the level of risk by considering the category of probability or likelihood against the category of consequence severity.
Risk Owner	Role or function with the accountability and authority to manage the risk.
Risk Profile	The set of risks or risk categories considered by an organisation that can hinder or disrupt the achievement of the strategic objectives.
Risk Register	Used to record and document the risk assessment process.
Risk Tolerance	The maximum amount of risk that an entity can accept within the risk appetite without hindering the achievement of its strategic objectives or operating plan.
Risk Transfer	Refers to the transfer of the consequence of a risk to another party through legislation, contract, insurance or other means. It can also refer to a shifting of a physical risk.
Risk Treatment	'The process of selection and implementation of measures to modify risk.'[12]
Risk Treatment Action Plan	Documents the process to be carried out for the development and implementation of risk treatments. They should contain: the tasks to be completed and the risks they address, the name of the task owners who have responsibility for implementation of treatment risks and a timetable for implementation.
Risk Treatment Owners	Role or function with the accountability and authority to manage the treatment of risk.
Shared Risks	Risks if not treated by one entity, become risks for other entities or risks that impact more than one entity.
Territory Authority	Refers to a body established for a public purpose under an Act, but does not include a body declared by regulation not to be a Territory authority.[13]
Territory Entity	A territory authority or a public sector company.[14]

IDENTIFY THE RISKS

APPENDIX A

What is the major CIT objective to be achieved?	*[This could be a core business function, or a project outcome]*
What is the key project/activity related to this objective that is being considered?	
What are the major threats or opportunities to the achievement of this particular activity/project? *CIT has identified the following elements as the possible sources for most of our risks. Consider these areas when answering this question. (not all may be relevant to this particular project/activity):*	
Business processes and systems	
Commercial/legal relationships (e.g. contracts)	
Financial management	
Staffing resources	
Staff skills	
Physical resources e.g. building, equipment etc.	
Technology	
Natural events	
Safety issues	
Fraud	
Customer/stakeholder and staff attitudes	
Security	
Other	
What are the possible areas that may be affected by risk? Consider the following:	
Tangible assets and resource base cost, both direct and indirect e.g. buildings, computers, furniture and fitouts etc.	
Intangible assets Individuals (the skills, knowledge and attributes of the organisation's employees – or individual know-how) Organisational (processes, systems, methodologies, brand/logo) External (customer relationship, supplier relationship, reputation etc.)	
Stakeholder management Who does this include? What impacts on our reputation with these stakeholders (that is, meeting their expectations and objectives)? What can we do to handle these stakeholder expectations?	
Our image and reputation	
Budget	
Legislation	
Performance Timeliness of activity	
Privacy and security	
Safety	
Insurance premiums	
Quality of services/products	

Probity Governance and transparency of decision making	
Are there any other factors that are likely to impact upon achievement of key objectives and outcomes? For example: ▪ contestability for services ▪ integration with work by other business units	

ANALYSE THE RISKS APPENDIX B

ACTIA - [ACT Government Risk Matrix]

ACTIA
Australian Capital Territory Insurance Authority

ACT Government

Last Update: 8 January 2019

Please see over the page for more consequences

	Consequence **				
	Insignificant	Minor	Moderate	Major	Catastrophic
Financial	1% of Budget or <$5K	2.5% of Budget or <$50K	> 5% of Budget or <$500K	> 10% of Budget or <$5M	>25% of Budget or >$5M
People	Injury or ailments not requiring First Aid treatment and / or psychological injury managed by staff support services.	Minor injury or requiring First Aid treatment or short term injury (less than four weeks incapacity for work) and / or psychological injury resulting in reduced ability to perform tasks requiring treatment from a health professional.	Serious injury causing hospitalisation or medium term reversible disability (four weeks or more incapacity for work) or multiple medical treatment cases and / or psychological injury resulting in reduced ability to perform tasks requiring ongoing support from GP/health professional.	Single life threatening injury (including loss of limbs) or multiple serious injuries causing hospitalisation and/or permanent disability and / or psychological injury resulting in reduced ability to perform tasks requiring significant additional psychological treatment.	Death or multiple life threatening injuries and/or multiple injuries causing major life altering impairment and / or psychological injury resulting in inability to perform tasks requiring ongoing significant psychological treatment.
Compliance/ Regulation	Non-compliance with work policy 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 require self reporting to the appropriate regulator and immediate rectification.	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.
Reputation & Image	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 Govt or Public Service forcing changes to the machinery of Govt.
Service Delivery	Loss of or interruption to non critical/no-core services up to 3 days.	Interruption of core services affecting critical infrastructure (e.g. law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days.	Cessation of core services affecting critical infrastructure (e.g. law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days and/or disruption for a week.	Cessation of core services affecting critical infrastructure (e.g. law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days and/or disruption over subsequent weeks.	Total cessation of core services affecting critical infrastructure (e.g. law & order, public safety, health) or cessation of core/ critical service essential to business continuity for more than 1 week and/or disruption over subsequent months.

Likelihood of Consequence	Frequency			Matrix	1	2	3	4	5
	Almost Certain	Is expected to occur in most circumstances	Once in a quarter or more	5	Medium	High	High	Extreme	Extreme
	Likely	Will probably occur	Once a year or more	4	Medium	Medium	High	High	Extreme
	Possible	Might occur at some time in the future	Once every 1 - 5 years	3	Low	Medium	Medium	High	Extreme
	Unlikely	Could occur but doubtful	Once every 5 - 20 years	2	Low	Medium	Medium	High	High *
	Rare	May occur but only in exceptional circumstances	Once every 20 - 100 years	1	Low	Low	Medium	Medium	High *

Priority for Attention / Action *				
Priority	Indicative Escalation	Indicative Action Plan	Authority for Action	Optional Considerations
Extreme	Within 24 hours	1 month or sooner	DG & DDG (CEO or equivalent)	Chair ARMC Director WH&S
High	Within 7-14 days	2 months or sooner	Senior Executive or equivalent (DDG/ED/Head of Agency or equivalent)	Director WH&S
Medium	Within 1-3 months	3 months or sooner	Executive/Business Unit Head/Manager	WH&S Team
Low	1-3 months in course of normal business	3-6 months or sooner	Team Leader/Supervisor	WH&S Team

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 consequence. Nothing further to be done except review and monitor the existing controls. Controls are largely preventative and management believes that they are effective and reliable at all times.
Room for Improvement	Some deficiencies in controls have been identified how ever 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 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.

* Priority for Attention / Action
Every care should be taken to act as soon as possible to implement risk control measures wherever possible or to take action to fix the problem. 'Extreme' and 'High' risks especially where the risk relates to people and personal injury require us to act immediately to take steps to fix the problem.
The suggested timing of treatment does not mean that immediate action ought not be taken or that the timing can not be completed sooner than suggested.

** Hint
To help assess the consequence and likelihood of a risk:
1. Consequence- What will be the outcome/impact should the risk eventuate in the most normal form? Where there are many consequences, choose the one that has the highest outcome/impact.
2. Likelihood- What is the likelihood of that outcome/impact?
3. When identifying, analysing and rating risk, consideration should be given but not necessarily limited to the above categories of risk and the suggested examples of frequency and consequences.

ACTIA

Category of risk	Consequence of risk in the most normal form				
	Insignificant	Minor	Moderate	Major	Catastrophic
Assets	Loss or destruction of assets up to $2,000.	Loss or destruction of assets $2,000 to $10,000.	Loss or destruction of assets $10,000 to $100,000.	Loss or destruction of assets $100,000 to $5M.	Loss or destruction of assets greater than $5M.
Compliance / Regulation	Non-compliance with work policy 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 require self reporting to the appropriate regulator and immediate rectification.	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.
People	Injury or ailments not requiring First Aid treatment **and/or** psychological injury managed by staff support services.	Minor injury or requiring First Aid treatment or short term injury (less than four weeks incapacity for work) **and/or** psychological injury resulting in reduced ability to perform tasks requiring treatment from a health professional.	Serious injury causing hospitalisation or medium term reversible disability (four weeks or more incapacity for work) or multiple medical treatment cases **and/or** psychological injury resulting in reduced ability to perform tasks requiring ongoing support from GP/health professional.	Single life threatening injury (including loss of limbs) or multiple serious injuries causing hospitalisation and/or permanent disability **and/or** psychological injury resulting in reduced ability to perform tasks requiring significant additional psychological treatment.	Death or multiple life threatening injuries and/or multiple injuries causing major life altering impairment **and/or** psychological injury resulting in inability to perform tasks requiring ongoing significant psychological treatment.
Environment	Limited effect to something of low significance and/or effects are limited to a small area with rapid recovery.	Transient, minor effects and/or minor effects to environment and/or disturbance of native vegetation or waterways.	Moderate, short-term environmental harm to environment and/or disturbance of native vegetation or waterways.	Significant, medium-term environmental harm to environment and/or disturbance of native vegetation or waterways.	Long term environmental harm and/or widespread or severe impacts to environment, threatened species and/or long term effects on ecological community or native vegetation or waterways.
Financial	1% of Budget or <$5K	2.5% of Budget or <$50K	>5% of Budget or <$500K	> 10% of Budget or <$5M	>25% of Budget or >$5M
Service Delivery	Loss of or interruption to non critical/no-core services up to 3 days.	Interruption of core services affecting critical infrastructure (eg law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days.	Cessation of core services affecting critical infrastructure (eg law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days and/or disruption for a week.	Cessation of core services affecting critical infrastructure (eg law & order, public safety, health) or cessation of core/ critical service essential to business continuity for up to 3 days and/or disruption over subsequent weeks.	Total cessation of core services affecting critical infrastructure (eg law &order, public safety, health) or cessation of core/ critical service essential to business continuity for more than 1 week and/or disruption over subsequent months.
Information & Records Management	Interruption to ICT systems, electronic records and data access less than ½ day and/or system breach to business administration system with no personal or classified information stored.	Interruption to ICT systems, electronic records and data access 1/2 - 1 day and/or system breach to business administration system with some identifiable information but non-client threatening (data access known).	Significant interruption (but not permanent loss) systems and data access 1-7 days and/or system breach to business administration system with some identifiable information but non-client threatening (data access unknown).	Complete, permanent loss of some electronic records and/or data, or loss of access to ICT systems and data for more than 7 days and/or systems breach to business administration system with identifiable/classified information stored but non-client welfare threatening.	Complete, permanent loss of or inability to recover/reconstruct all records and data and/or total loss of confidence in data/record integrity and/or systems breach to Govt or business critical systems with client and/or business welfare threatened.
Reputation & Image	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 Govt or Public Service forcing changes to the machinery of Govt.
Cultural & Heritage	Low-level repairable damage to commonplace structures.	Mostly repairable damage to items of cultural and/or heritage significance.	Significant damage to items of cultural and/or heritage significance.	Permanent damage to structures or items of cultural and/or heritage significance.	Irreparable damage to or loss of highly valued items of cultural and/or heritage significance.
General Business Activities	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 and/or negligible disruption to services or non-essential subsidiary services.	Policy procedural rule occasionally not met and/or services do not fully meet need and/or minor impact on business outcomes and strategic objectives and/or non-essential 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. Unable to deliver necessary critical services.

CIT Risk Matrix

Likelihood	Consequence				
	Insignificant ①	Minor ②	Moderate ③	Major ④	Catastrophic ⑤
Almost Certain ⑤	Medium	High	High	Extreme	Extreme
Likely ④	Medium	Medium	High	High	Extreme
Possible ③	Low	Medium	Medium	High	High
Unlikely ②	Low	Medium	Medium	Medium	High
Rare ①	Low	Low	Low	Medium	Medium

Note: Multiplying the likelihood and the consequence will assist in prioritising the risk.

Risk Response

Rating	Required Response/Timeframe
Extreme **20 – 25 hrs**	• Preferred treatment options: avoid, transfer or mitigate (insurance, contractor). • Requires immediate escalation and active management through continual monitoring. Review treatment strategies systematically to determine their adequacy and effectiveness against the required outcomes. • Further controls are needed unless impractical or financially non-viable. • Report to Executive, specific management response required within 24 hours
High **10 – 16 hrs**	• Preferred treatment options: avoid, transfer or mitigate. • Requires escalation through routine reporting and active management through systematic monitoring. Review treatment strategies routinely to determine their adequacy and effectiveness against the required outcomes. • Additional controls may be required to protect CITs interests and business. • Report to Senior Management at Director level, specific management response required within 48 hours.
Medium **4 – 9 hrs**	• Preferred treatment options: mitigate or accept. • Manage by specific monitoring or response procedures, with clear management responsibility. • Watching Brief, Notify management at HOD level, update risk assessment, specific management response within one week.
Low **1 – 3 hrs**	• Preferred treatment options: accept. • Manage by routine processes, review and re-evaluate within 3 months.

Likelihood

Rating	Likelihood of the risk occurring in the next 3 years	
	Description	**Estimated probability**
Almost Certain	Almost certainly will occur, or has occurred in the past	>90%
Likely	Is likely to occur in the current operational environment.	61 - 90%
Possible	Will possibly occur in the current operational environment.	21 - 60%
Unlikely	Is unlikely to occur in the current operational environment.	2 - 20%
Rare	May occur in rare circumstances only.	<2%

Consequence

Level	Operational	Legal/Compliance	Safety & Wellbeing
Catastrophic	**Continuity of service**: Disruption to : >10% clients for : >24 hours; OR **Business interruption**: severe and/or long term (> 6 months) disruption or delay on an element of operations.	Breach of law with severe consequences such as prosecutions, litigation, severe fines, and/or licence to operate suspended.	Death (eg, suicide, fatality) or serious self-harm or permanent psychological disability, irreversible disability or mental health condition. Long term absence from the workplace – eg >12 months. Permanent or profound negative impact on health at work and/or work capacity Serious negative impact on other staff, work area and/organisation as a whole.
Major	**Continuity of service**: Disruption to : ≥10% clients for : <24 hours OR **Business Interruption**: Major and/or medium term (1-6 months) disruption or delay on an element or operations.	Breach of law with major consequences such as litigation, fines, extensive reporting. external audit regimes imposed and/or licence to operate reviewed by regulator.	Extensive injuries, impairment, long term (years) recovery and medical intervention. Significant self-harm, long term psychological disability or mental health condition. Medium-long term absence from the workplace – eg, 6-12 months. Long term or significant negative impact on health at work and/or work capacity Significant negative impact on other staff, work area and/organisation as a whole. Multiple Compensation claim for psychological injury.
Moderate	**Continuity of service**: Disruption to <10% of customers for <24 hours; OR **Business Interruption**: Moderate and/or short – medium term (>2 weeks- 1 month) disruption delay on an element of operations.	Breach of law with moderate consequences such as investigations, threat of litigation, moderate fines, government and regulator notifications requiring remedial action, breach of licence or authorisation conditions, additional reporting and/or internal audit requirements imposed.	Safety: medium term (months) reversible disability. Medical intervention required, long term psychological disability or mental health condition. Medium term absence from the workplace – eg,3-6 months. Moderate or medium term negative impact on health at work and/or work capacity Moderate or medium term negative impact on other staff, work area and/organisation as a whole. Compensation claim for psychological injury.
Minor	**Continuity of service**: Disruption to <10% of customers for <12 hours; OR **Business Interruption**: Minor and/or short term (days-<2 weeks) disruption or delay on an element of service.	Breach of law with minor consequences such as non-compliances or legal issues, regulator notifications, fines and/or reporting.	Short term (weeks) reversible disability or illness. First aid treatment required. Minor self-harm, short term or minor term psychological or mental health condition. Short term absence from the workplace – eg,<3 months. Short term or minor negative impact on health at work and/or work capacity Short term or minor negative impact on other staff, work area and/organisation as a whole. Possible compensation claim for psychological injury.
Insignificant	Insignificant and/or short term (days) disruption or delay on an element of operations.	Breach of law with limited effects and/or breaches or regulations.	Injury or aliment associated with swift recovery. No treatment required. Single or minor psychological or mental health issues that have no impact on health at work or work capacity. Infrequent absenteeism. No impact on other staff, work area and/or organisation as a whole.

EVALUATE RISKS APPENDIX C

Criteria Against Which To Evaluate Risks

The higher the overall level of risk the greater level of management attention is required to reduce its likelihood and/or impact or manage the risk. We recommend the following approach be taken:

Extreme Risk	High Risk	Medium Risk	Low Risk
Possible courses of action	**Action required**	**Some action may be required**	**Action may not be required**
• Treatment required within one month • Detailed action plan required • Extreme risks require urgent CEO and Board Chair attention. They are unacceptable without mitigating controls. • All risks assessed as Extreme should be reported to the Audit, Risk and Finance Committee.	• Treatment normally within three months • High risks should only be accepted following consultation with the Chief Executive Officer and in the absence of cost effective mitigations • The effectiveness of existing controls and planned treatment strategies should be reviewed bi-annually in consultation with the Chief Executive Officer. The decision to accept a high risk should also be reviewed as part of this consultation	• Treatment within one year • Moderate risks may be acceptable in the absence of cost effective mitigations. Management responsibility as specified • Moderate risks should be reviewed annually as part of risk management planning to determine whether the risk identification and analysis remain aligned with the operating environment	• Low risks are acceptable and may be managed by routine procedures • Low risks should be reviewed annually as part of risk management planning to determine whether the risk identification and analysis remain aligned with the operating environment

Control Effectiveness	Guide
Adequate	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, are largely preventative and address the root causes and Management believes that they are effective
Room for improvement	Most Controls are designed correctly and are in place and effective however there are some control that are either not correctly designed or are not very effective. There may be an over reliance on reactive controls. Some more work to be done to improve operating.
Inadequate	Significant control gaps or no credible control. Either controls do not treat root causes or they do not operate effectively. Controls if they exist are just reactive. Management has no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness.

CIT RISK MANAGEMENT TEMPLATE APPENDIX D

#	Risk	Risk Sources and Impacts	Current Risk Treatment Strategies (Existing Controls)	Current Risk (Controls in place)	Accept risk?	Planned Risk Treatment Strategies (Controls Not Yet Implemented)		Target Risk (after new risk treatments)
						Description	Owner Timeframe (and status)	
1.		Sources Impacts:		Consequence: Likelihood: Risk Rating:				Consequence: Likelihood: Risk Rating: