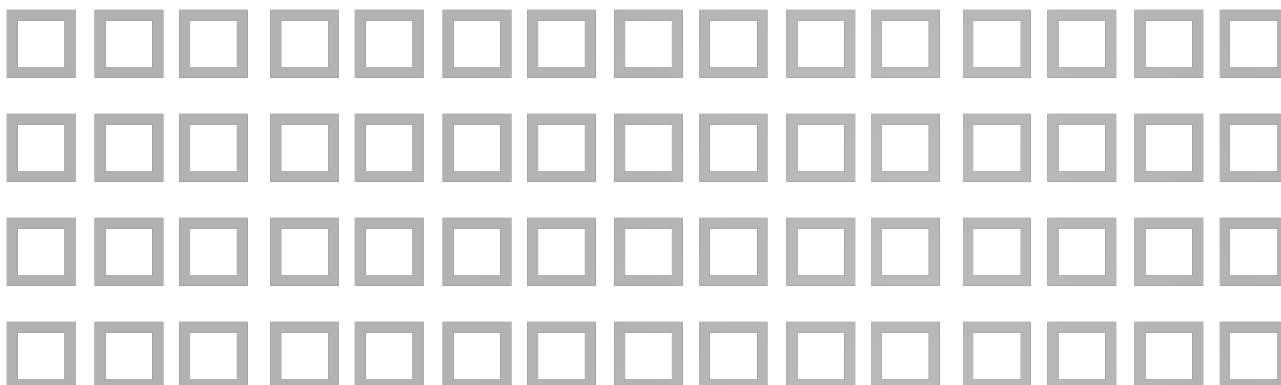


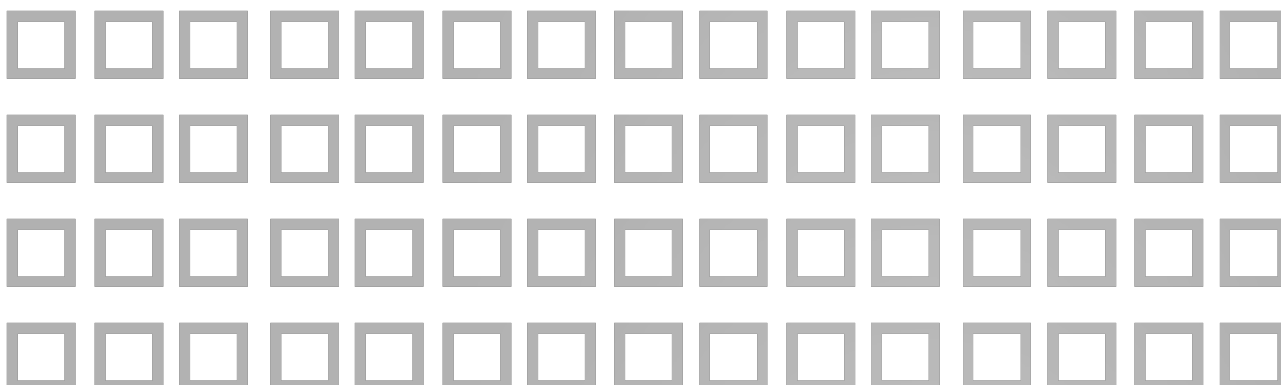
Elections ACT

ACT ELECTORAL COMMISSION OFFICERS
OF THE ACT LEGISLATIVE ASSEMBLY



ACTEC Risk Management Plan

October 2020



Accessibility

Elections ACT is committed to making its information and services accessible to as many people as possible.

- If you have difficulty reading a standard printed document and would like to receive this publication in an alternative format – such as large print or audio – please telephone 02 6205 0033.
- If English is not your first language and you require the translating and interpreting service – please telephone 13 14 50.
- If you have a hearing or speech impairment, contact us through the National Relay Service:
 - TTY users phone 133 677 then ask for 02 6205 0033
 - Speak and Listen users phone 1300 555 727 then ask for 02 6205 0033
 - Internet relay users connect to NRS (www.relayservice.com.au) and then ask for 02 6205 0033
- ACT Interpreter Service – for the deaf and blind – please telephone 02 6287 4391.

Contents

Introduction	1
Purpose	1
Scope	2
Tools	2
Risk Management Process	3
Risk Assessment – Developing Risk Registers	4
1. <i>Communication and Consultation</i>	4
2. <i>Establishing the Scope, Context and Criteria</i>	5
3. <i>Risk Assessment</i>	5
4. <i>Risk Treatment</i>	7
5. <i>Monitoring and Review</i>	7
6. <i>Recording and Reporting</i>	8
Activities Supported by this Risk Management Plan	9
<i>Internal Audit</i>	9
<i>Business Continuity Management</i>	9
<i>Fraud and Corruption Prevention</i>	9
<i>Senior Executive Responsible for Business Integrity Risk (SERBIR)</i>	10
<i>Workplace Health and Safety</i>	10
<i>Training and Support</i>	11
Conclusion	11
Attachment A – Part 1 – ACT Government Risk Assessment Matrix	12
Attachment B – Guidelines for developing a Risk Management Plan for a Project	16
<i>Components of a Risk Management Plan (RMP)</i>	16
Attachment C - ACTEC Project and Program Risk Matrix Template	18

Introduction

Purpose

The Australian Capital Territory Electoral Commission (ACTEC) is committed to effective and efficient identification, treatment and monitoring of risks to the organisation. Oversight of risk management processes are undertaken by the Commissioner and the Commission.

The ACTEC 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 Risk Plan are to:

- provide a detailed guide to support the effective implementation of the ACTEC Risk Management Framework and Policy Statement;
- outline the risk management process to be followed;
- minimise the exposure to significant risks through the identification, assessment; management, monitoring, review and reporting of risk; and
- enhance the 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 taking action to avoid or reduce the chances of something going wrong;
- 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 proactive 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;
- 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 ACTEC Risk Management Plan (the Plan) establishes the processes for risk management in ACTEC. 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 ACTEC.

This Plan is consistent with the AS/NZS ISO 31000:2018 Risk Management – Guidelines standard. Territory entities must ensure that they comply with this Standard.

Tools

ACTEC has a number of documents and tools for conducting risk assessments and the ongoing management of risks. The following table identifies and describes the aforementioned documents and tools and distinguishes responsibility for the associated actions.

Table 1 – Risk Management Tools supporting the risk assessment process

Tool	Description	Responsibility
Risk Management Framework & Policy Statement, and Risk Management Plan	Application of the ACTEC Risk Management Framework and Policy Statement and this risk management plan. Establishment of a Risk Management Plan pertaining to the project	Senior Management and Team Leaders Project Manager
Risk Registers	The Risk Register enables staff to document, manage, monitor, review and update strategic, corporate and operational risk information. For each risk the following will be captured: <ul style="list-style-type: none"> ▪ the risk category; ▪ a description of the risk event; ▪ the causes 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 of the risk owner; ▪ the existing controls being relied upon; ▪ the name(s) of the control owner(s); ▪ the control effectiveness (CE); and ▪ the risk rating. 	Senior Management and Team Leaders Project Managers and project teams

Risk Treatment Action Plans	<p>Information from the risk management process is recorded, reported and monitored using the Risk Register.</p> <p>A Risk Treatment Action Plan will be prepared for all 'high' and 'extreme' rated risks.</p> <p>Risk Treatment Action Plans will contain:</p> <ul style="list-style-type: none"> the tasks to be completed and the risks they address; the name of the task owners who have responsibility for implementation of treatment tasks; and the timetable for implementation. 	<p>Senior Management and Team Leaders</p> <p>Project Managers and project teams</p>
Training	Ongoing training and development for relevant team staff to ensure that the team is equipped with sound risk management knowledge and skills base.	Senior Management and Team Leaders
Reporting	<i>Refer to Reporting section following for details.</i> Risk reports draw information from the risk registers and allows management to monitor and review risks in alignment with the strategic plan, operational plans, and other cascading plans.	<p>Senior Management and Team Leaders</p> <p>Project Managers</p>

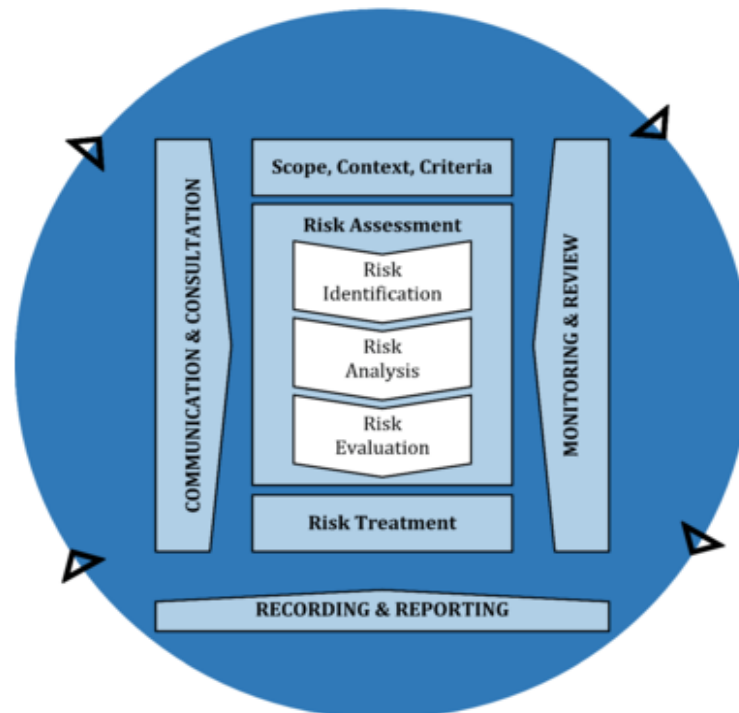
Risk Management Process

Risk management is an iterative 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 ACTEC and risks should be managed according to: the ACTEC Risk Management Framework and Policy Statement; 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 scope, context and criteria;
3. risk assessment (including identification, analysis and evaluation);
4. risk treatment;
5. monitoring and review; and
6. recording and reporting.

Diagram 1 – The risk management process as set out in the AS/NZS ISO 31000:2018 risk management guidelines 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 ACTEC in order to achieve the overall objectives of the entity. 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 throughout the risk management process 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.

Communication and consultation is an integral part of risk management that should be repeated throughout each step of the risk management process.

2. Establishing the Scope, Context and Criteria

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 ACTEC has established its risk criteria and they are contained in **Attachment A** 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. Guidelines for developing a Risk Management Plan for a Project can be found at **Attachment B**. Note that these guidelines also include a template for an ACTEC Project and Program Risk Matrix, at **Attachment C**.

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. ISO 31000:2018 observes the below with respect to comprehensively identifying risks that may impact on an organisation:

"The following factors, and the relationship between these factors, should be considered:

- tangible and intangible sources of risk;
- causes and events;
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risks;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge and reliability of information;

¹ ISO Guide 73:2009 at paragraph 3.5.1

- time-related factors;
- biases, assumptions and beliefs of those involved.

The organization should identify risks, whether or not their sources are under its control..."²

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 approach 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"***.³

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.

² ISO 31000:2018 – 6.4.2 Risk Identification

³ ISO Guide 73:2009 at paragraph 3.6.1

4. Risk Treatment

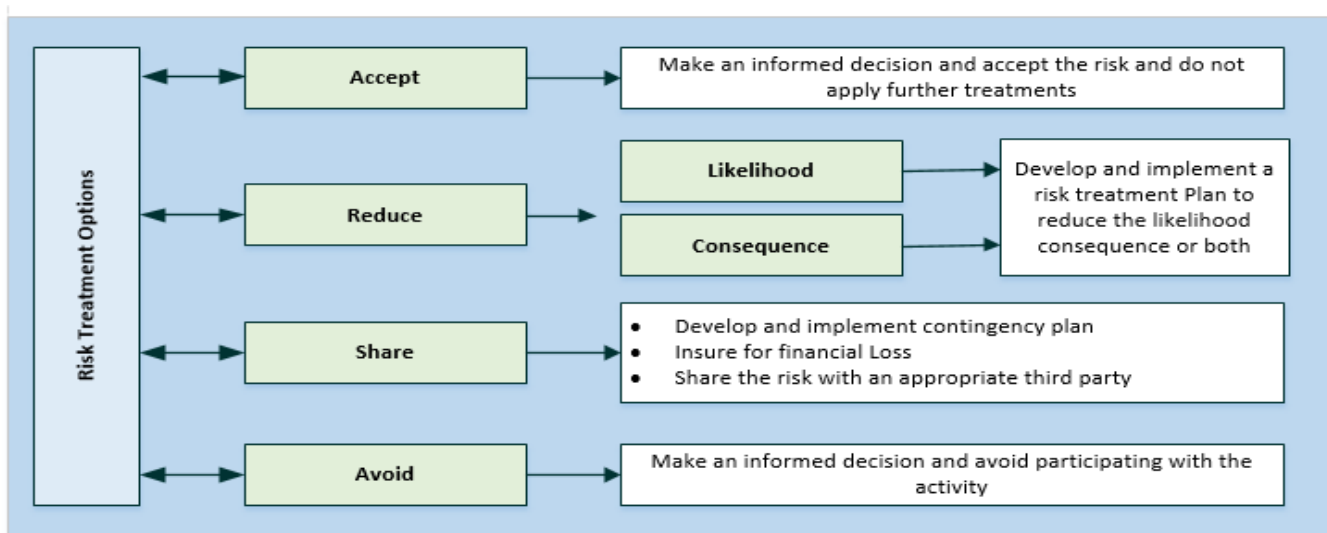
Treatment of risk involves selecting one or more options for modifying the risk or managing the risk to a status acceptable within the entity's risk tolerance. This process will generally include developing and implementing specific strategies and action plans for increasing potential benefits and improving outcomes to manage the risk. To improve the management of controls and treatments the use of SMART methodologies is recommended.

- 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)

Using the SMART methodology, provides a mechanism to test the control and report the effectiveness of the control to the risk owner.

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 treatment mechanisms.



5. Monitoring and Review

The risk management process is iterative 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 effectiveness 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.

6. Recording and Reporting

6.1 Recording and Maintenance

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

Risk registers should be reviewed as per the following timeline:

- annually by the Electoral Commissioner;
- annually by Elections ACT or as determined as part of the business and strategic planning process will be revised to reflect the further actions required to be taken to comply with these principles; and
- projects are to conduct reviews of existing risks on a regular basis in accordance with normal project management requirements– set out in the risk management plan that relates to the project.

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

6.2 Reporting

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

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.

Internal Audit

The Internal Audit Program has been developed in part on the basis of the Strategic Risk Register and ACTEC 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 is integral to ACTEC's overall risk management framework and reflects the organisation's commitment to sound risk management and corporate governance practices. 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 (BCPs).

The purpose of the ACTEC BCPs 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 challenges associated with accommodation, information and communications technology and personnel. The BCP analyses and records potential business impacts, recovery priorities and risk management strategies. The BCPs also describe 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 ACTEC Risk Manager is responsible for coordinating the development, monitoring, testing and review of the ACTEC BCP documentation.

Fraud and Corruption Prevention

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

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 Integrity Policy for the ACT Public Service sets out the broad whole of government policy on the promotion of integrity in the ACT Public Service. The *Public Sector Management Standards 2016* detail the formal responsibilities of agencies to promote integrity and to control fraud and corruption. The ACTEC Fraud Corruption and Prevention Plan 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. The *Public Sector Management Standards 2016* require that the process be repeated every two years. In addition, existing plans and procedures must be reviewed in the light of any significant breaches of the policies or any substantive program or organisational change.

Senior Executive Responsible for Business Integrity Risk (SERBIR)

In accordance with the *Public Sector Management Standards 2016* (at section 113), certain provisions of the *Public Sector Management Standards 2006* (repealed) (for example section 14(7)) continue to apply. As a result, the Electoral Commissioner 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 ACTEC is the Deputy Electoral Commissioner. The SERBIR is a 'champion' of integrity in ACTEC and promotes awareness and acceptance of the ACTPS Integrity Policy and the organisations' Fraud and Corruption Prevention Plan. The SERBIR is also responsible for regularly reporting on overall compliance with the relevant policies to the Commission

Workplace Health and Safety

The ACTEC values its 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. The ACT Public Service is committed to the health and wellbeing of the individuals that make up our workforce and the individuals that come into our workplaces to access government services. Workplace safety awareness and robust risk management practice aim to ensure that our workplaces are safe, thus reducing incidents of death, injury and disease.

ACTEC 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 Plan provides the processes for risk management that apply 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 which 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, has been developed and will be maintained in order to meet ACTEC's obligations under the *Work Health and Safety Act 2011*.

Training and Support

This Plan, in conjunction with the ACTEC Risk Management Framework and Policy Statement, is 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 achieve risk management maturity across ACTEC, regular risk management training is made available to all staff. Additional risk management training may be accessed by staff through the ACT Government training calendar and by the ACT Insurance Authority.

Conclusion

ACTEC is responsible for the delivery of fair and open elections and referendums, in addition to the provision of high quality electoral information, education, advice and services to the ACT Community. To this end, its approach to managing risks to its operations can be seen to have three principal areas of focus:

- a risk management platform of defined guidelines and accountabilities supported by risk management tools and templates;
- a business practice approach to risk management integrated in operation management at all levels including business, project and resource planning and reporting; and
- the identification and management of strategic risks by regular high-level review.

This Plan, in conjunction with the ACTEC Risk Management Framework and Policy Statement, is one of the key governance measures designed to ensure that risks are properly identified, assessed and managed. In practice, the Risk Management Framework and Plan must be seen as living documents, developing and evolving to reflect changing internal and external environments, and responding to new and previously unanticipated risks to the quality and effectiveness of its work.

It is expected that all staff will know, understand and support their defined role in the management of risks and in the development and application of this Plan.

Attachment A: Part 1 – ACT Government Risk Assessment Matrix

Attachment B: Guidelines for developing a Risk Management Plan for a Project

Attachment C: ACTEC Project and Program Risk Matrix Template

Attachment A – Part 1 – ACT Government Risk Assessment Matrix

	Frequency				Consequence					
						Insignificant	Minor	Moderate	Major	Catastrophic
					Matrix	1	2	3	4	5
	Almost Certain	Is expected to occur in most circumstances	Once a quarter or more	>1 in 10	E	Medium	High	High	Extreme	Extreme
	Likely	Will probably occur	Once a year or more	1 in 10 – 100	D	Medium	Medium	High	High	Extreme
Likelihood	Possible	Might occur at some time in the future	Once every 1-5 years	1 in 100 – 1,000	C	Low	Medium	Medium	High	Extreme
	Unlikely	Could occur but doubtful	Once every 5 – 20 years	1 in 1,000 – 10,000	B	Low	Medium	Medium	High	High
	Rare	May occur but only in exceptional circumstances	Once every 20 – 100 years	1 in 10,000 – 100,000	A	Low	Low	Medium	Medium	High

	Suggested Timing of Treatment	
Extreme	Short term – normally within one month** Detailed action plan required	Electoral Commissioner Electoral Commission
High	Medium term – normally within three months Needs senior management attention	Deputy Electoral Commissioner
Medium	Normally within 1 year Specify management responsibility	Managers
Low	Ongoing control as part of a management system Manage by routine procedures	All Staff

Control Effectiveness	Guide
Adequate	Nothing more to be done except review and monitor the existing controls. Controls are well designed. Management believe that they are effective.
Room for Improvement	Some controls are either not correctly designed or are not very effective. More work needs to be done.
Inadequate	Significant control gaps or no credible control.

Categories of Risk	Consequence					
		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 that 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 that threaten business delivery	Operations shut down by regulator for failing to comply with relevant guidelines and /or significant non-compliance with internal procedures could result in failure to provide business outcomes and service delivery
	People	Injuries or ailments not requiring medical treatment	Minor injury or First Aid Treatment Case	Serious injury causing hospitalisation or multiple medical treatment cases	Life threatening injury or multiple serious injuries causing hospitalisation	Death or multiple life threatening injuries
	Environment	Limited effect to something of low significance	Transient, minor effects	Moderate, short-term environmental harm	Significant, medium-term environmental harm	Long term environmental harm
	Financial	1% of Budget	2.5% of Budget	> 5% of Budget	> 10% of Budget	>15% of Budget
	Service Disruption	Very minimal disruption to services, of less than 1 month	Minor to moderate disruption to services for up to 1 month	Total cessation of service for up to 1 day and subsequent disruption of 1 to 2 months	Total cessation of service for up to 7 days and subsequent disruption of 2 to 3 months	Total cessation of service for more than 1 week and disruption over subsequent months involving a major facility
	Technology	Interruption to electronic records and data access less than ½ day.	Interruption to electronic records and data access ½ to 1 day	Significant interruption (but not permanent loss) to data and electronic records access, lasting 1 day to 1 week	Complete, permanent loss of some electronic records and/or data, or loss of access for more than one week	Complete, permanent loss of all electronic records and data

	General management activities	Minimal impact on business objectives. Minor delays for non-essential services	Minor impact on business outcomes and strategic objectives. Non-essential or subsidiary services experience delays and service disruptions	Moderate impact on business outcomes and strategic objectives. A number of objectives not met, minor or subsidiary services impaired	Significant impact on business and strategic objectives. Key service delivery impaired	Strategic business outcomes processes fail and business objectives not met. Unable to delivery necessary services
	Reputation & Image	Internal Review	Scrutiny required by internal committees or internal audit to prevent escalation	Scrutiny required by external committees or ACT Auditor General's Office, or inquest, etc.	Intense public, political and media scrutiny. E.g.: front page headlines, TV, etc.	Assembly inquiry or Commission of inquiry or adverse national media
	Cultural & Heritage	Low-level repairable damage to commonplace structures	Mostly repairable damage	Significant damage to structures or items of cultural significance	Permanent damage to items of cultural significance	Irreparable damage to highly valued items of cultural significance
	Business Process & Systems	Minor errors in systems or processes requiring corrective action, or minor delay without impact on overall schedule	Policy procedural rule occasionally not met or services do not fully meet needs	One or more key accountability requirements not met. Inconvenient but not client welfare threatening	Strategies not consistent with Government's agenda. Trends show service is degraded	Critical system failure, bad policy advice or ongoing non-compliance. Business severely affected

Attachment B – Guidelines for developing a Risk Management Plan for a Project

Projects undertaken by ACTEC are required to establish a Risk Management Plan (RMP) and Risk Register at the time of inception.

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

Components of a Risk Management Plan (RMP)

A 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 Project.

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

Introduction

- RMP Purpose
 - To manage the actions of identifying, assessing and treating risks to the project objectives and the resulting deliverables.
 - To create, maintain and report upon the risk register.
- Identify the intended audience.

Objectives and scope of the risk management plan

- General – risk is to be managed:
 - In accordance with the AS/NZS ISO 31000:2018 Risk Management - Guidelines standard.
 - The ACTEC Risk Management Framework and Policy Statement.
- Risk management objectives
 - To broadly identify and appropriately treat and manage risks affecting project objectives (the context for the risk assessment).
- The risk criteria
 - The criteria to be used in the risk assessment – the ACT Government risk management matrix tailored to the constraints of the project.
Also refer to **Attachment C - ACTEC Project and Program Risk Matrix Template.**

The risk management organisation and reporting structures

- Roles and responsibilities
 - Identify all roles that have responsibilities that include risk management and outline those responsibilities.
- Resources
 - Identify and outline the resources available for risk management, budget and control
- Structure
 - Including relationships with stakeholders outside the project boundary

Risk assessment

- Communication and consultation
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment

Risk management monitoring and review

- Arrangements for risk monitoring including the authority for acceptance and continued tolerance of risks
- Risk Reviews
 - Frequency and arrangements for periodic reviews, reviews relating to milestones and other reviews.
- Risk Reporting
 - Nature, frequency and recipients of the risk management reports.
 - Co-ordination with other related projects that will affect the successful delivery of each.

Risk register

- 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
- The most current version of the risk register can be attached to the RMP.

Attachment C - ACTEC Project and Program Risk Matrix Template

Likelihood	Frequency				Consequence					
					Matrix	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
	Almost Certain	Is expected to occur in most circumstances	Once a quarter or more	>1 in 10	E	Medium	High	High	Extreme	Extreme
	Likely	Will probably occur	Once a year or more	1 in 10 – 100	D	Medium	Medium	High	High	Extreme
	Possible	Might occur at some time in the future	Once every 1-5 years	1 in 100 – 1,000	C	Low	Medium	Medium	High	Extreme
	Unlikely	Could occur but doubtful	Once every 5 – 20 years	1 in 1,000 – 10,000	B	Low	Medium	Medium	High	High
	Rare	May occur but only in exceptional circumstances	Once every 20 – 100 years	1 in 10,000 – 100,000	A	Low	Low	Medium	Medium	High

	Suggested Timing of Treatment	Authority for the continued tolerance of risk		
		Program	Project	Organisational
Extreme	Short term – normally within one month** Detailed action plan required			Director- General Under-Treasurer
High	Medium term – normally within three months Needs senior management attention			Senior Executive
Medium	Normally within 1 year Specify management responsibility			Managers
Low	Ongoing control as part of a management system. Manage by routine procedures			All staff

Control Effectiveness	Guide
Adequate	Nothing more to be done except review and monitor the existing controls. Controls are well designed. Management believe that they are effective.
Room for Improvement	Some controls are either not correctly designed or are not very effective. More work needs to be done.
Inadequate	Significant control gaps or no credible control.

Categories of Risk	Consequence					
		Insignificant	Minor	Moderate	Major	Catastrophic
	Assets	Loss or destruction of assets up to \$_____	Loss or destruction of assets \$_____ to \$_____	Loss or destruction of assets \$_____to \$_____	Loss or destruction of assets \$_____ to \$_____	Loss or destruction of assets greater than \$_____
	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 and /or significant non-compliance with internal procedures could result in failure to provide business outcomes and service delivery.
	People	Injuries or ailments not requiring medical treatment.	Minor injury or First Aid Treatment Case.	Serious injury causing hospitalisation or multiple medical treatment cases.	Life threatening injury or multiple serious injuries causing hospitalisation.	Death or multiple life threatening injuries.
	Environment	Limited effect to something of low significance	Transient, minor effects	Moderate, short-term environmental harm	Significant, medium-term environmental harm	Long term environmental harm
	Financial	1% of Budget	2.5% of Budget	> 5% of Budget	> 10% of Budget	>15% of Budget
	General management activities	Minimal impact on business objectives. Minor delays for non-essential services.	Minor impact on business outcomes and strategic objectives. Non-essential or subsidiary services experience delays and service disruptions.	Moderate impact on business outcomes and strategic objectives. A number of objectives not met, minor or subsidiary services impaired.	Significant impact on business and strategic objectives. Key service delivery impaired.	Strategic business outcomes processes fail and business objectives not met. Unable to delivery necessary services.
	Reputation & Image	Internal Review	Scrutiny required by internal committees or internal audit to prevent escalation.	Scrutiny required by external committees or ACT Auditor General’s Office, or inquest, etc.	Intense public, political and media scrutiny. E.g.: front page headlines, TV, etc.	Assembly inquiry or Commission of inquiry or adverse national media.
	Cultural & Heritage	Low-level repairable damage to commonplace structures	Mostly repairable damage	Significant damage to structures or items of cultural significance	Permanent damage to items of cultural significance	Irreparable damage to highly valued items of cultural significance
Key Project Delivery	Delays Less than 2 weeks	Delays 2 to 4 weeks	Delays 4 to 6 weeks	Delays 6 to 10 weeks	Delays Greater than 10 weeks	

Note: The Project and Program Risk Matrix above should be tailored to the particulars of the project or program for which the risk assessment is to be undertaken.