Australian Government | acma

Australian Communications and Media Authority

Standard Operating Procedure – Risk Management Process

AUGUST 2024

This **Standard Operating Procedure – Risk Management Process** applies to all officials of the ACMA including Authority and Associate Members, the eSafety Commissioner and all ACMA staff, including staff that assist the eSafety Commissioner in eSafety roles and functions.

INTERNAL DOCUMENT	
Approved by	Executive Manager Research, Data, Regulation and Governance
Contact officer	Manager Performance, Governance, Audit and Risk
Date	August 2024
Next review	August 2025

Contents

1. Introduction 4

1.1 Scope 4

1.2 Complying with this SOP 4

2. Risk Management in the ACMA 4

2.1 Risk Management Framework 4

2.2 Why do we have a Risk Management Process? 5

2.3 How does Risk Management relate to me? 5

2.4 When do I undertake a Risk Assessment? 5

3. Risk Management Process 6

3.1 Overview 6

3.2 Establishing the Scope, Context and Criteria 7

3.3 Risk Assessment 7

3.3.1 Risk Identification 8

3.3.2 Risk Analysis 9

3.3.3 Risk Evaluation 10

3.4 Risk Treatment 11

3.5 Recording and Reporting 12

3.6 Communication and Consultation 12

3.7 Monitoring and Review 13

4. Summary of Related Information 14

Appendix A – Tables and Diagrams 15

A.1 Likelihood Table 15

A.2 Consequence Table 16

A.3 Risk Matrix 18

A.4 Inherent, Current and Residual or Target Risk 19

A.5 Current Risk Level and Response 20

A.6 Mapping the Risk Management Process against the Template 21

Document Control

Version control

Version	Date	Description	Approved
0.1	May 2024	Initial draft	Executive Manager – Research, Data, Regulation and Governance
1.0	August 2024	Reviewed and cleared by the Executive Management Committee	Chair

Change control

The Manager, Performance, Governance, Audit and Risk (PGAR) is responsible for maintaining and updating this document.

1. Introduction

1.1 Scope

This Standard Operating Procedure (SOP) provides operational guidance on the ACMA's risk management process, including the method for conducting a risk assessment.

This SOP is to be read in conjunction with the other documents in the ACMA Risk Management Framework (see 2.1 below).

1.2 Complying with this SOP

All ACMA officials must comply with this SOP.

Paragraph 6(2)(c) of the *Australian Communications and Media Authority Act 2005* (ACMA Act) provides that 'ACMA officials' are officials of the ACMA. Section 3 of the ACMA Act defines an 'ACMA official' to mean:

- a member
- an associate member
- a member of the ACMA staff[1]
- a person whose services are made available to the ACMA under subsection 55(1).[2]

Under subsection 184(3) of the *Online Safety Act 2021*, the ACMA must make available members of staff to assist the eSafety Commissioner to perform their functions and exercise their powers. All officials who are assisting eSafety for the purpose of this SOP are ACMA officials and must comply with this SOP. In addition, under section 170 of the *Online Safety Act 2021*, the eSafety Commissioner is an official of the ACMA for the purposes of the finance law.

Contractors (including consultants) and other third parties undertaking duties on behalf of the ACMA or eSafety are, generally, obliged under their contract to comply with all Commonwealth laws and policies, declare conflicts of interest and not act fraudulently. If they breach their contract conditions, they may incur sanctions or remedies under the contract or they may become subject to legal proceedings.[3] Accordingly, contractors (including consultants) and other third parties should also comply with this SOP.

2. Risk Management in the ACMA

2.1 Risk Management Framework

The ACMA's Risk Management Framework (Framework) supports effective decision-making and creates a shared understanding of our risks, including controls and treatments. The Framework is designed to identify our risks transparently and systematically through

[1] Section 54 of the ACMA Act states that ACMA staff are to be persons engaged under the *Public Service Act 1999.*

[2] Section 55 of the ACMA Act allows for the services of officers or employees of other Commonwealth entities, companies or bodies established for a public purpose under Commonwealth law to be made available for the purposes of the ACMA.

[3] Australian Government Contract Management Guide January 2020 Version 1.3.

standardised processes.

The Framework includes the following documents:

- The Risk Management Policy - sets out the risk management approach, including the overall intentions and directions for risk management, and defines the risk appetite and tolerance.
- Accountable Authority Instruction – Risk Management – instructions on duties and responsibilities relating to risk management.
- This **Standard Operating Procedure – Risk Management Process**
- Risk Management Plan Template – which includes:
  - a **Risk Register Template** - to record the results of a risk assessment.
  - a **Risk Treatment Plan Template** - to record the future actions to be taken to address identified risks.

Officials should refer to the other documents in the Framework for further guidance on risk management.

2.2 Why do we have a Risk Management Process?

The risk management process aims to embed risk management into the culture and work practices of the ACMA, to facilitate well-informed decision making, maximise opportunities and manage threats. The risk management process is designed to add value, ensure accountability, and improve the ACMA's overall operations.

2.3 How does Risk Management relate to me?

Everyone has a role in risk management because it is integral in all that we do.

All business areas should engage in risk management in their daily work. ACMA officials need to understand the relevance of risk management, and how to use the ACMA's Risk Management Framework including this SOP to apply risk management.

As explained in the Risk Management Policy (section 1.1), the Framework applies to organisational risk, and guidance including other SOPs for different areas can assist staff in applying risk management to specific regulatory functions.

2.4 When do I undertake a Risk Assessment?

The Risk Management Process detailed in this SOP includes undertaking a risk assessment. The ACMA's Risk Management Plan Template contains a risk register template to be used for recording the outcome of a risk assessment.

However, not everything we do requires us to complete a risk assessment. The need for a risk assessment should be determined on a case-by-case basis.

In general, a risk assessment is required where:

- there is a legislative or regulatory obligation to complete a risk assessment, or
- undertaking programs or projects, particularly where these relate to the achievement of an ACMA activity linked to a Corporate Plan priority and/or where there is a commitment

of financial or people resourcing required to achieve an ACMA outcome, or

- the function or activity may expose the ACMA to financial loss, fraud or corruption, or security risks or where the health and safety of people may be threatened, or
- the function or activity may involve contact with children (people under 18) by ACMA officials or parties connected to the ACMA (see the ACMA and eSafety Child Safety Policy for more information), or
- new or innovative business activities or processes are being designed, or
- existing processes are altered in a way that may alter the effectiveness of controls, or
- there has been a material change in the ACMA's operating environment, or
- a new activity or a modification to an activity is being considered that will affect either internal or external ACMA stakeholders.

3. Risk Management Process

3.1 Overview

The ACMA risk management process is consistent with the international standard *AS ISO 31000:2018 Risk management – Guidelines*. The process is summarised below, with each stage expanded in following sections.

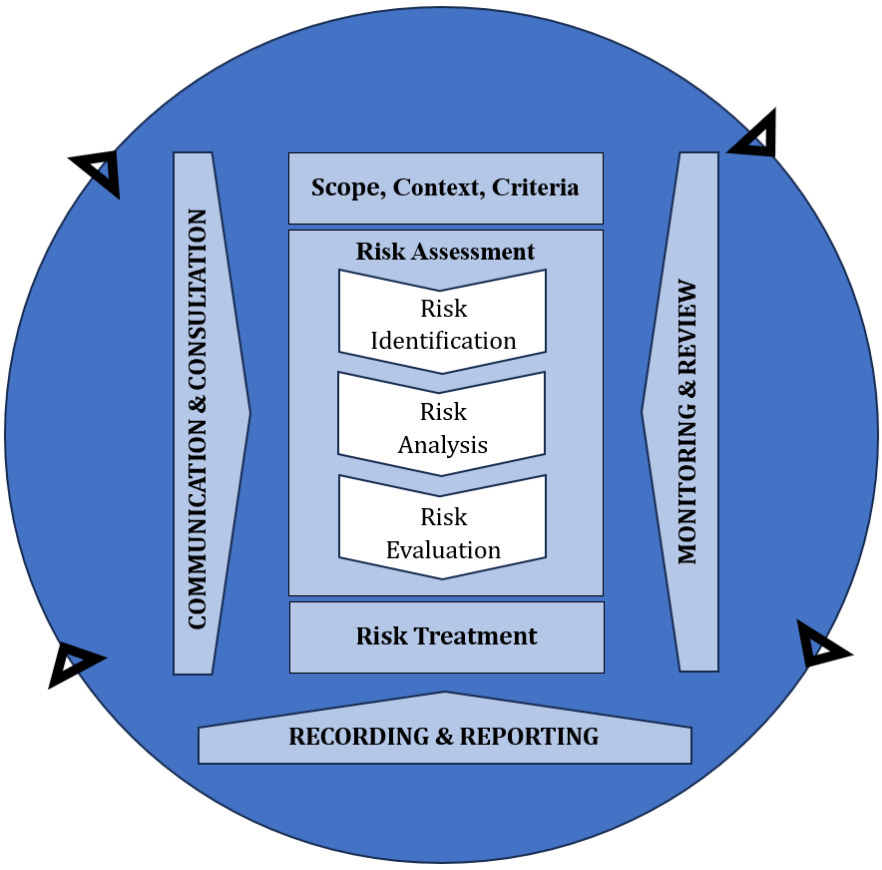


Figure 1: Risk Management Process

In addition, Appendix A.6 of this SOP maps the risk management process against the Risk Management Plan template, to further assist officials make and record decisions.

3.2 Establishing the Scope, Context and Criteria

Establishing the scope, context and criteria is important to ensuring that the risk assessment is effective and that any treatments are appropriate.

Defining the scope includes considering:

- the objective(s) to be achieved and decisions to be made
- whether the risks being managed are strategic, enterprise, divisional, discrete, or shared (see Risk Management Policy, sections 3.2 to 3.6)
- stakeholder needs
- expected outcomes
- times, locations, inclusions, and exclusions
- resources required
- relationships with other projects, processes, or activities
- confirming who will be advised of the risk assessment, including which boards or committees (if any) will have oversight.[4]

Understanding the context involves considering the environment in which we operate, including internal and external factors, such as:

- the social, political, legal, and regulatory landscape
- stakeholders
- involvement of children
- business continuity, climate, and disaster risks
- national health risks
- organisational structure, roles, and accountabilities
- internal policies, procedures, and culture
- capabilities, budgets, and available resources.

Criteria includes considering the amount and type of risk that the ACMA is willing to take to achieve our strategic objectives, as defined in our Risk Appetite and Tolerance statements (see Risk Management Policy, sections 5.1 and 5.2). Many other criteria are defined in the attachments to this SOP, which detail how we measure likelihood and consequence, the risk matrix that we use to define risk levels, and the response to risk at each level.

3.3 Risk Assessment

Risk assessment is the process of risk identification, risk analysis and risk evaluation.

It is recommended that a risk assessment is conducted by at least two or three people working together, to allow for broader input that can lead to better assessment of risks. Workshops or other meetings may be used to help ensure all relevant perspectives are considered as part of the risk assessment.

[4] Relevant boards or committees could include a Divisional Digital Board, the Enterprise Project Group, or the Executive Management Committee.

The risk register template should be used to record the outcomes of risk assessments. Guidance is included in the template to assist with completion.

Where appropriate, other risk templates or methods may be authorised for use by the official, board or committee providing oversight of the risk assessment. These instances may include specialised risk assessments, or assessments to suit a project methodology or Commonwealth requirements. In addition, ACMA policies may also authorise the use of other risk templates. For example, the ACMA Fraud and Corruption Control Policy allows the use of templates provided by the Commonwealth Fraud Prevention Centre when conducting a fraud and corruption risk assessment.

3.3.1 Risk Identification

Risk identification is the stage of finding, recognising, and describing risks. Risk identification involves discovering the areas of uncertainty and the potential events that may affect the achievement of your objectives.

The focus of risk identification should be on events with the greatest potential impact on the delivery of the objectives. To focus on the objectives, the following questions could be asked as part of the identification process:

- what must go right to meet our objectives?
- what information is vital to our success?
- with a severely limited budget, where would you spend your first dollar?
- what tools and assets are vital to the objectives?

A starting point can be the creation of a list of events that might affect objectives. Consider negative effects or threats (e.g. delaying, degrading, or preventing objectives) and positive effects or opportunities (e.g. creating, enhancing, or accelerating objectives and outcomes).

Risk identification should include:

- describing the source or cause of the risk
- confirming the risk is within scope (that it relates to the achievement of objectives)
- determining the risk owner[5] for each risk
- considering whether there are risks associated with conflicts of interest and the acceptance or provision of gifts, benefits, and hospitality.[6]

Risk identification should also include consideration of whether an activity involves contact with children by ACMA officials or another party connected to the ACMA. If any child safety risks are identified, a specific child safety risk assessment must be undertaken. Contact the PGAR team for information regarding child safety risk assessments by emailing risk@acma.gov.au.

Stakeholder input and feedback is important at the risk identification stage. Broad input ensures that a greater variety of risks can be identified, and allows stakeholders the ability to engage with risks and commit to risk ownership where required.

Several techniques can be used to identify risks, including but not limited to:

[5] See Risk Management Policy, chapter 9 for the definition of risk owner.

[6] See the ACMA Conflicts of Interest Policy and Official Hospitality and Business Catering Guide.

- structured workshops
- environmental scanning
- SWOT analysis
- business process mapping
- analysis of complaints or past events
- scenario analysis
- obtaining expert advice
- audits or investigations.

Officials should use any or all techniques that are suited to the area or activities subject to the risk assessment, and those that are most accessible and understood by the participants.

Risks should be identified whether the ACMA can modify them or not. Even if the ACMA cannot stop a particular risk event from happening, some corrective controls or treatments to assist with recovery or minimising harms may be put in place.

A useful way of describing a risk is to explain an event or situation in terms of what could happen or not happen, or what is present and what it could lead to regarding the ACMA's objectives. The following is a general approach to describing risk:

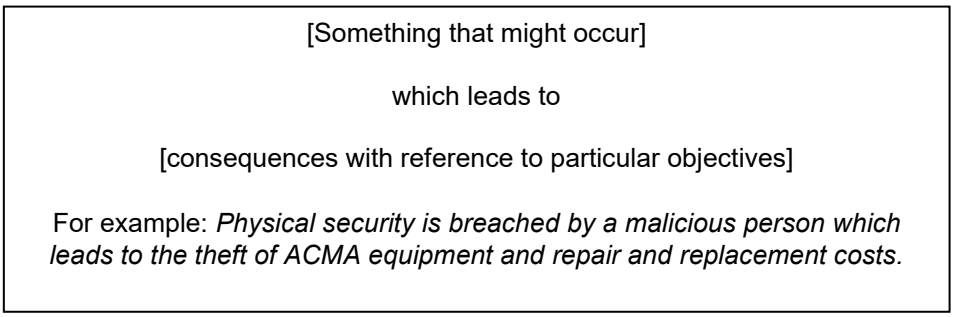


Figure 2: General Approach to Describing Risk

3.3.2 Risk Analysis

The purpose of risk analysis is to understand the nature of the risks, and determine the level of risks by considering the likelihood and consequences of the risks. The effectiveness of existing controls (see Risk Management Policy, chapter 6) is also considered in the analysis.

Likelihood is the chance of something happening, or how probable it is for a risk event to be realised. Likelihood is measured in percentages and over time. Where possible, historical or quantitative information should be used to establish likelihood. The ACMA uses a five-scale assessment of likelihood, from rare to almost certain (as shown in Appendix A.1).

Consequence is the potential outcome or impact of a risk event. The ACMA classifies consequences as negligible, minor, moderate, major, or severe (as shown in Appendix A.2). When assessing consequence, officials should consider the level of impact in relation to the categories from the consequence table. For example, a risk may have a major consequence for financial, and moderate for reputation and stakeholder management. Both ratings may be recorded, as this demonstrates that consideration of the risk has been thorough.

Once the likelihood and consequence are established, each risk should be plotted against the ACMA's risk matrix to determine its risk level (see Appendix A.3). The rating associated

with each level can be used in the ACMA risk register template to assist in the further consideration of risks.

Officials should also determine the relevant risk appetite that applies to each risk. The risk appetite for some categories of risk is found in the Risk Management Policy (section 5.1). In other cases, risk appetite can be determined from other internal documents such as SOPs.

There is value in considering the speed of onset of a risk as well. Risks that can be realised quickly or without warning pose a greater threat to the ACMA. These risks may need stronger controls and more monitoring than risks which unfold slowly and allow us more time to react.

During the analysis stage, you should also consider the controls that are in place, and the effectiveness of the controls (see Risk Management Policy, chapter 6). You may require assistance or advice from the control owners to determine whether controls are effective.

The risk register template allows risks to be analysed and rated at three stages:

- inherent risk (before controls are considered)
- current risk (the present state with controls in place but without future treatments)
- residual or target risk (after the treatments have been implemented).

The inherent and current risk should be rated and recorded during the analysis stage.

See Appendix A.4 for a diagram showing how to determine inherent, current, and residual or target risk.

3.3.3 Risk Evaluation

Risk evaluation involves comparing the results of the risk analysis with relevant criteria to determine where additional actions (or treatments) are required.

Evaluation also includes comparing the identified risks against each other, to determine which risks are the priority. Typically, risks with the highest risk ratings have priority. It is recommended that risks are ordered in the risk register from the highest current risk rating to the lowest, as this gives prominence to the greatest current threats.

The Current Risk Level and Response chart provides indicative guidance for officials in evaluating appropriate responses to risks at each level from very low up to extreme (see Appendix A.5). Regarding approval levels, the chart specifies:

- **high risks** require the relevant Executive Manager to be briefed on the risk.
- **very high risks** require the relevant General Manager to be briefed on the risk.
- **extreme risks** require the General Manager to be advised immediately (or in the absence of the General Manager, officials are to notify the Office of the Chair).

Other considerations during evaluation include:

- is the current risk rating higher than acceptable? If so, treatments will be needed.
- is the risk outside risk appetite? If so, corrective action is required.
- is the escalation of any risks required? (see Risk Management Policy, section 5.3)

The decisions made should be recorded and endorsed by the risk owner and any other reviewing official or body, including relevant boards or committees.

Officials should also consider whether there are any emerging risks. These should be recorded in the 'risk environment scanning / consideration of emerging risks' section of the risk register and reported to relevant officials.[7]

3.4 Risk Treatment

Risk treatment is the process to select and implement actions to modify an identified risk until that risk is at an acceptable level.

Risk treatment is an iterative process as illustrated below:

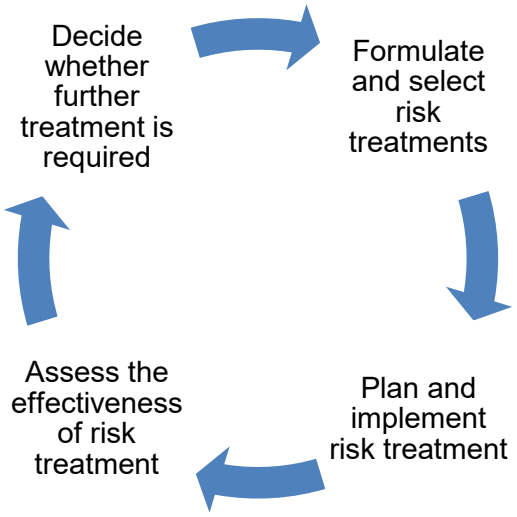


Figure 3: Risk Treatment Process

Formulating and selecting risk treatments involves balancing the proposed benefit of the treatment against the costs and resources required for its implementation.

Options for treating identified risks may involve one or more of the following:

- avoiding the risk by deciding not to start or continue the activity
- removing the source of the risk
- reducing the likelihood and/or consequences of the risk
- accepting the risk without further action
- transferring part of the risk to another party (through contracts or insurance).

While risks can be transferred in part through contracts or insurance, this option should be relied upon in limited circumstances. It is possible that, as a government agency, the ACMA may retain the ultimate responsibility for any risk events that might occur.

In the context of delivering a program or project, establishing a governance body such as a project board or steering committee can help manage risk. Factors which may influence the

[7] See Risk Management Policy, chapter 7 for further information on the management of emerging risks.

establishment of a governance body include:

- the scale and complexity of the program or project
- the stability of the operating environment
- the extent that the program or project relates to strategic priorities
- the extent that the program or project impacts internal or external ACMA stakeholders.

Agreed treatments should be recorded in the risk treatment plan section of the Risk Management Plan after affected stakeholders are consulted. Potential stakeholders could include the risk owner, the person or team tasked with implementing the treatment, and the owners of existing controls. Progress on risk treatments should be regularly reported to the risk owner.

Where additional treatments are planned (or in progress), the person or group conducting the risk assessment must consider how the risk will be affected by those treatments. A treatment owner and timeframe should be recorded for each treatment.

Consideration must also be given to the residual or target risk that is expected after the treatments will be implemented, and whether this is within risk appetite and tolerance. If the risk will remain outside of appetite and tolerance after treatment, then it must be escalated.

After a treatment has been implemented in full, it is often considered to be a control. At that time, the implemented treatment can be removed from the treatment plan and added as a control in the risk register section of the Risk Management Plan.

3.5 Recording and Reporting

Recording and reporting involves providing evidence for the outcomes of risk assessments and the decisions made.

Risk registers and risk treatment plans are the primary method for recording and reporting risk assessments and subsequent treatments to support informed decision making. These documents as contained in the Risk Management Plan are designed to present a balanced assessment of the potential outcomes of an activity or project. It is the responsibility of the person or body providing approval to ensure a risk assessment has been completed and recorded before the activity or project proceeds.

The level of oversight required is dependent on the type of risk being assessed. ACMA officials recorded as risk owners must keep the risk registers updated and notify the person, board, or committee performing oversight of any significant changes to the risk.

Officials should refer to the Current Risk Level and Response chart in Appendix A.5 for relevant approval levels for high, very high, and extreme risks.

3.6 Communication and Consultation

ACMA officials should communicate and consult with relevant internal and external stakeholders during all steps of the risk management process.

Communication seeks to promote awareness and understanding of risk. Consultation involves obtaining feedback and information to support decision-making. Together,

communication and consultation assist stakeholders to understand risk, the basis on which decisions are made, and the reasons why certain actions are required.

It is important for ACMA officials to consult with colleagues who may be affected by the decisions that they make. This internal consultation ensures that different views are considered and helps to foster a sense of inclusiveness among those officials who may be affected by the decisions.

Consultation with external stakeholders can allow for appropriate input from experts, build consensus regarding treatments, and support transparency in decision-making.

3.7 Monitoring and Review

Monitoring and review can provide assurance and improve the quality and effectiveness of process implementation and outcomes. Monitoring and review should occur at all stages of the risk management process.

To ensure that new risks are identified, and existing risks are appropriately managed, risk owners are to check individual risks within their business area on a regular basis (at least every six months). A process of ongoing discussion about risk, including working groups and peer moderation, is important to ensure a consistent approach.

Key considerations of monitoring and review include:

- changes in the internal and external operating environment
- appearance of new risks
- further information to improve the understanding of previously identified risks
- effectiveness of controls
- implementation of treatments
- learning from successes and failures
- identification of ‘near misses’ or unsatisfactory risk management.

The ‘risk environment scanning/ consideration of emerging risks’ section of the risk register can be updated to record this information.

The results of monitoring and review should be incorporated into reporting activities, including in reports provided to relevant boards or committees.

In addition, the following aspects of monitoring and review also should be reported back to the PGAR team at risk@acma.gov.au:

- **value add** – the degree to which risk management contributes to the achievement of the team, division, or agency objectives, and its effectiveness in identifying and managing risk
- **maturity** – whether the risk management framework is fit-for-purpose for the team, division or entity
- **compliance** – the extent and the consistency of the application of the risk management framework in practice across the team, division, or entity.

The information gathered will inform the regular review of the Risk Management Framework that is conducted by the PGAR team.

4. Summary of Related Information

Summary of related information	
Legislative requirements	PGPA Act: s.15, s.16, s.19, s.40, s.41, s.42, s.43, s.44, s.45 PGPA Rule: s.17 *Auditor-General Act 1997*: s.32
Policies of the Australian Government	Commonwealth Risk Management Policy
Guidance	Resource Management Guide (RMG) 131: Developing performance measures RMG 132: Corporate plans for Commonwealth entities Guide for non-corporate Commonwealth entities on the role of audit committees RMG 211: Implementing the Commonwealth Risk Management Policy RMG 214: Notification of significant non-compliance with finance law
Related AAIs	Risk Management Fraud and Corruption Control Audit
Internal delegations	All financial and people delegations are posted on the Hub.
Other relevant documents	These are listed under Risk Management Framework in section 2.1 of this SOP.
Contacts	Manager, Performance, Governance, Audit and Risk Risk@acma.gov.au

Appendix A – Tables and Diagrams

A.1 Likelihood Table

The ACMA uses a five-scale assessment of likelihood, from almost certain to rare:

Almost certain	Over 80% chance of happening; occurs on a regular basis; or could occur within days to weeks.
Likely	Between 50% and 80% chance of happening; has occurred several times before; or could occur within weeks to months
Possible	20% to 50% chance of happening; has occurred once or twice before; or could occur in a year or so.
Unlikely	5% to 20% chance of happening; has not happened before but could; or could occur every few years.
Rare	Less than 5% chance of happening; conceivable but only in exceptional circumstances; or could occur once every 10 or more years.

Table 1: ACMA likelihood table

A.2 Consequence Table

The consequence table provides 5 defined ranges of consequences for 6 categories

Threats						
	Category	**Negligible**	**Minor**	**Moderate**	**Major**	**Severe**
Regulatory	**Trust (Public confidence in communications and media services)**	No public impact.	Few public concerns with media and communications services.	Competing and contrary voices in the environment undermine Government policy and program delivery	Ongoing disruption to communications and media services.	Failure of communications and media services results in complete loss of confidence.
	Systems and infrastructure (Spectrum management benefits all Australians)	Trivial or no impact on spectrum.	Australia's international standing as a leader in wireless technology uses is diminished	Legal challenge to its spectrum management decisions delays spectrum allocations and rollouts of new wireless and satellite technologies	Spectrum is not allocated and used efficiently or effectively, disrupting communications networks	Failure of spectrum management.
	Systems and infrastructure (A regulatory framework that anticipates change in dynamic communications and media markets)	Insignificant market impact.	Markets underperform due to outdated regulation	Regulation fails to keep pace with market innovation	Market failure results from uncontrolled market innovation	Market failure that affects ongoing viability of the industry or the ACMA.
Organisational	**Trust (Reputation and stakeholder management)**	No impact on stakeholder relationships. No damage to ACMA's reputation.	Issues resolved through routine management practices.	Consultation or engagement required by legislation or Commonwealth policy.	Issues requiring management at Chair/Authority level or involvement of Minister.	Grave or irreversible damage to reputation and relationships.
	Financial	Financial variance of 2% or under.	3 to 5% variation in budget or event with a financial impact below $100,000.	6 to 10% variation in budget or event with a financial impact between $100,000 and $500,000.	11 to 25% variation in budget or event with a negative financial impact between $500,000 and $1 million.	Over 25% variation in budget or event with a financial impact over $1 million.
	Work Health and Safety	Injury that requires no first aid	Injury or illness requiring first aid.	Illness or injury requiring medical or	Injury or illness requiring long-term recovery	Illness or injury affecting multiple people

Threats						
	Category	Negligible	Minor	Moderate	Major	Severe
		treatment. Illness that needs no treatment.		professional medical treatment and short-term recovery.	and/or permanent disablement.	involving long term recovery, permanent disablement, and/or loss of life.

Table 2: ACMA consequence table

A.3 Risk Matrix

		CONSEQUENCE				
		Negligible	Minor	Moderate	Major	Severe
LIKELIHOOD	Almost certain	Medium	High	Very high	Extreme	Extreme
	Likely	Low	Medium	High	Very high	Extreme
	Possible	Low	Low	Medium	High	Very high
	Unlikely	Very low	Low	Low	Medium	High
	Rare	Very low	Very low	Low	Medium	Medium

Table 3: ACMA risk matrix

A.4 Inherent, Current and Residual or Target Risk

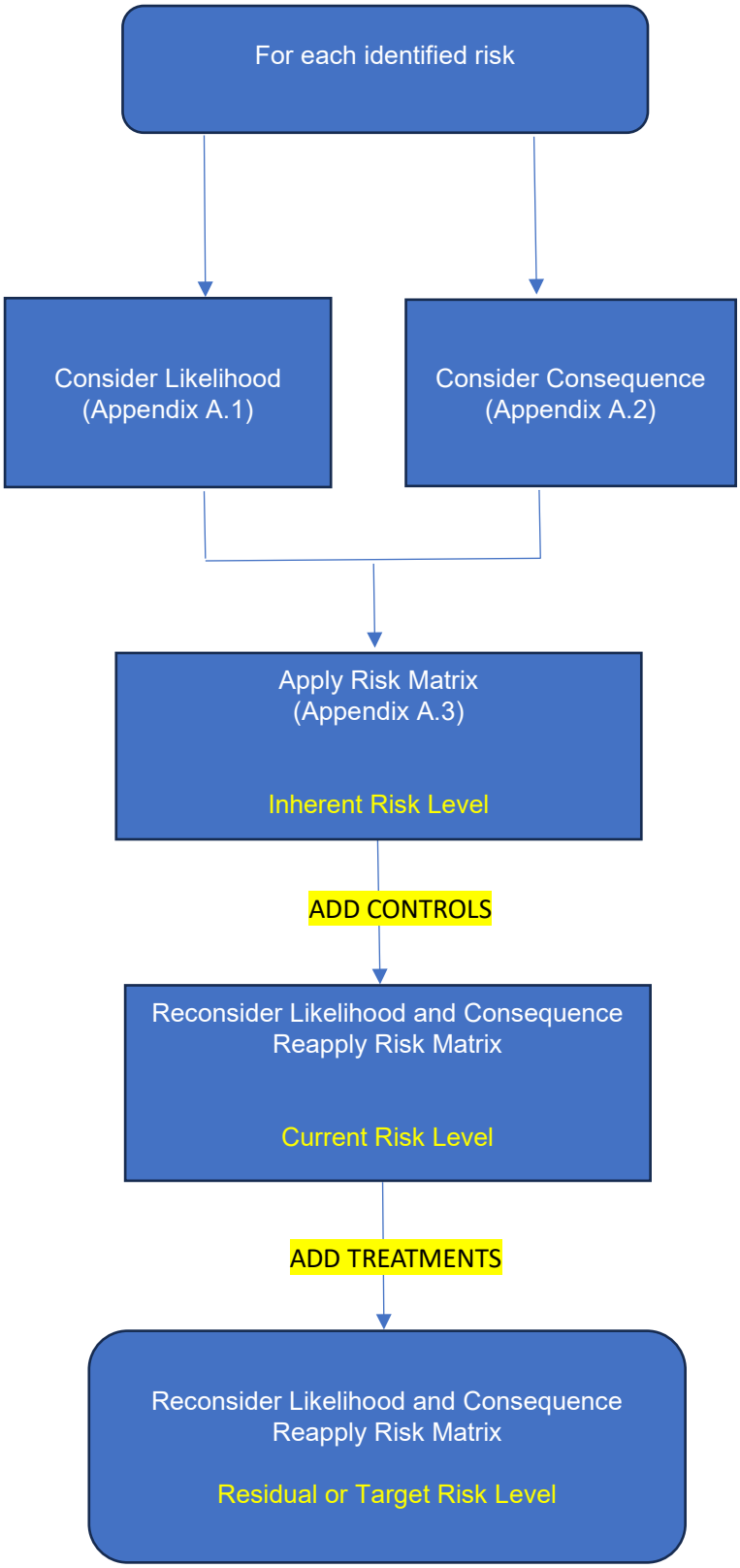


Diagram 1: Inherent, current, and residual or target risk

A.5 Current Risk Level and Response

Current Risk Level	Response
Extreme	• Risk is unacceptable. • Do not proceed with the activity (or cease if it is underway). • Seek advice of the relevant General Manager immediately. • In the absence of the General Manager, notify the Office of the Chair.
Very high	• Risk is unacceptable. • Reconsider whether the activity should be undertaken, including how it might be modified so that it is no longer very high risk. • Reduce consequence and/or likelihood through additional treatments immediately. • Take urgent action to improve effectiveness of all controls. • Undertake further analysis if needed to understand the risk. • Ensure that the relevant General Manager has been briefed on the risk, and endorses the commencement or continuation of the activity.
High	• Risk is unacceptable. • Reduce consequence and/or likelihood through additional treatments in the near future. • Take urgent action to improve effectiveness of critical controls. • Improve effectiveness of other existing controls that are rated less than strong or effective. • Undertake further analysis if needed to understand the risk. • Ensure that the relevant Executive Manager has been briefed on the risk, and endorses the commencement or continuation of the activity.
Medium	• Risk is acceptable, provided it is within appetite and tolerance. • Consider options to efficiently reduce consequence or likelihood through additional treatments. • Consider improving effectiveness of existing controls that are rated less than strong or effective.
Low	• Risk is acceptable. • Manage and monitor by routine internal procedures and maintenance of existing controls. • Consider the benefit of low-cost additional treatments to improve control effectiveness. • If no treatments need to be implemented, then risks where both inherent and current risk is low can be removed from the risk register.
Very low	• Risk is acceptable. No action needed. • Very low risks do not need to be recorded in the risk register.

Table 4: ACMA risk levels and response

A.6 Mapping the Risk Management Process against the Template

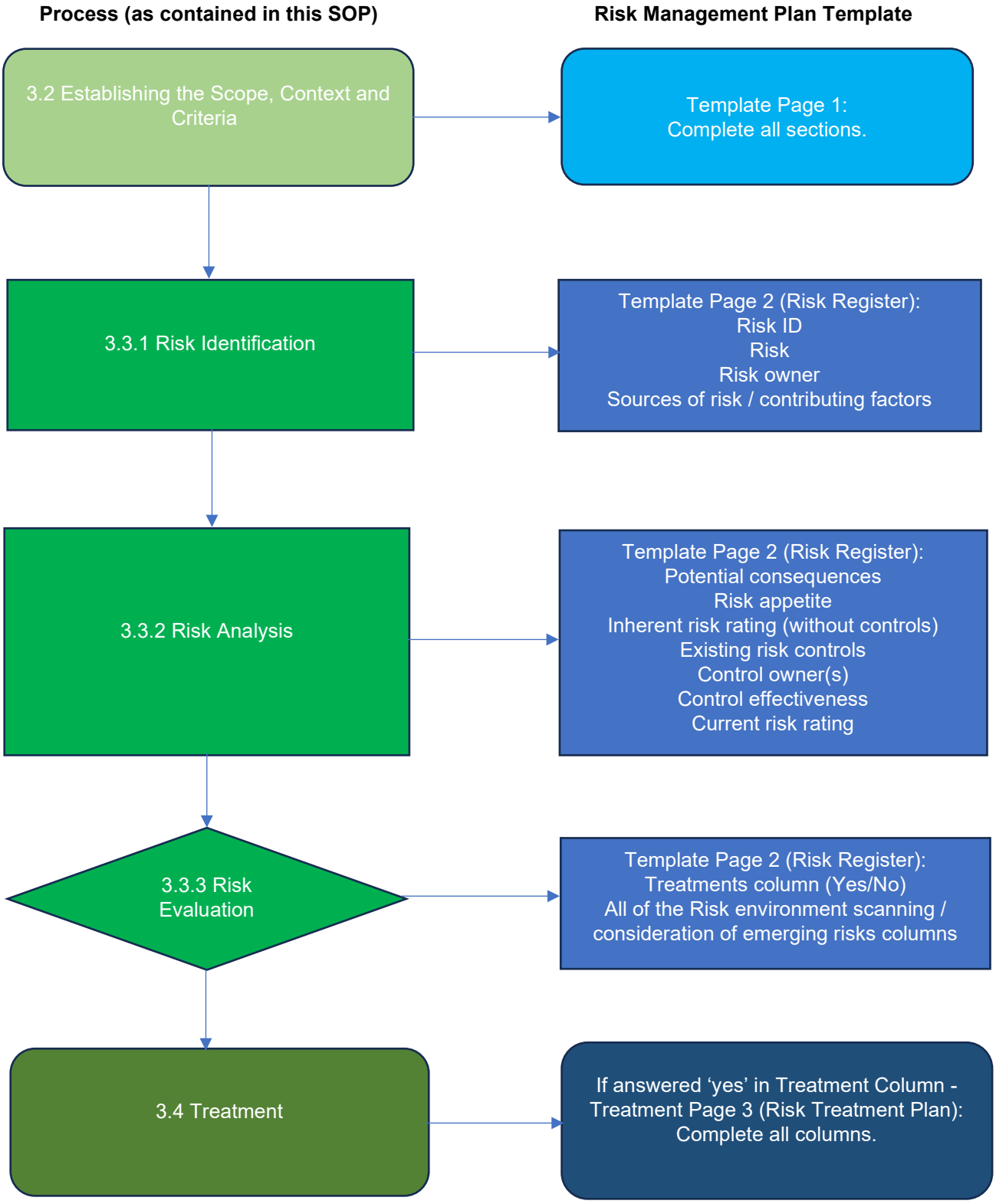


Diagram 2: Mapping the Risk Management Process Against the Template