Australian Government | acma Australian Communications and Media Authority

Risk Management Guide

Authorising officer

Chair and accountable authority
Australian Communications and Media Authority

Contact officer
Manager
Performance Governance Audit and Risk

Date
September 2026

Next review
September 2027

This Guide applies to ACMA staff, including Authority and associate members.

Contents

1 Introduction 4
1.1 About this Guide 4
1.2 Purpose 4
1.3 Complying with this guide 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 7
3.1 Overview 7
3.2 Scope, Context and Criteria 7
3.3 Risk Assessment 8
3.4 Rating risks 9
3.5 Risk Identification 10
3.6 Risk Analysis 11
3.7 Controls 12
3.8 Control effectiveness 12
3.9 Control testing 12
3.10 Risk Evaluation 13
3.11 Risk Escalation 14
3.12 Risk Treatment 15
3.13 Treatment Evaluation 17
3.14 Recording and Reporting 18
3.15 Communication and Consultation 18
3.16 Monitoring and Review 18
Appendix A – Tables and Diagrams 20
A.1 Mapping the Risk Management Process against the Template 20
A.2 Likelihood Table 21
A.3 Consequence Table 22
A.4 Risk Matrix 24
A.5 Inherent, Current and Residual or Target Risk 25
A.6 Current Risk Level and Response 26
A.7 Risk assessment escalation and treatment diagram 27

Document History

Version	Date	Description	Approved
01	September 2026	New Risk Management Guide replaces and updates the Standard Operating Procedure – Risk Management Process	
02			
03			
04			
05			

Change Control

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

1 Introduction

1.1 About this Guide

1.1.1 This Guide is issued in conjunction with the ACMA's (the entity's) Accountable Authority Instruction (AAI) on Risk Management.

1.1.2 This Guide has been designed to ensure that the entity complies with the requirements of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the*Public Governance, Performance and Accountability Rule 2014* (PGPA Rule).

1.1.3 This Guide provides entity officials with operational guidance on the ACMA's risk management process, including the method for conducting a risk assessment.

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

1.2 Purpose

1.2.1 The Guide provides the foundation for managing risk at the Australian Communications and Media Authority (ACMA). It supports effective decision-making and creates a shared understanding of risk management through tools and instructions to identify, assess, document, escalate, monitor and respond to risks. The Guide forms an integral part of the ACMA's corporate governance responsibilities.

1.2.2 This Guide aims to support ACMA staff with their risk management responsibilities and applies in all strategic, operational and project level activities. The purpose of the Guide is to:

- Define responsibilities and structures to ensure that risk management practices are incorporated into strategic, operational and project planning, and review processes.
- Promote an environment where decision makers can make informed decisions to identify and manage risks in an open and transparent manner.
- Create a risk culture where all staff assume responsibility for managing risk in their day-to-day activities.
- Ensure a consistent approach to risk management.

1.3 Complying with this guide

1.3.1 ACMA staff must comply with this Guide. This includes Authority members and associate members.

1.3.2 The eSafety Commissioner and staff assisting the eSafety Commissioner in performing the Commissioner's roles and exercising the Commissioner's functions, must comply with the eSafety Risk Management Guide.

2 Risk Management in the ACMA

2.1 Risk Management Framework

2.1.1 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 standardised processes.

2.1.2 The Framework consists of the following documents:

- **Accountable Authority Instruction** – Risk Management – instructions on duties and responsibilities relating to risk management.
- **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.
- **This Risk Management Guide.**
- **Risk Management Assessment – Cheat Sheet.**
- **Control Testing Guidelines.**
- **Risk Management Plan Template** – which includes:
  - Risk Register Template - to record the results of a risk assessment.
  - Risk Treatment Plan Template - to record the future actions to be taken to address identified risks.

2.1.3 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?

2.2.1 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?

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

2.3.2 ACMA officials need to understand the relevance of risk management, and how to use the ACMA's Risk Management Framework including this Guide to apply risk management.

2.3.3 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 Guide to apply risk management.

2.4 When do I undertake a Risk Assessment?

2.4.1 The Risk Management Process detailed in this Guide 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.

2.4.2 A documented risk assessment is not required for all our work. The need for a documented risk assessment should be determined on a case-by-case basis.

2.4.3 In general, a documented risk assessment is required where one or more of the following conditions are met:

- there is a legislative or regulatory obligation to complete a risk assessment
- 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
- 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

- 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)
- new or innovative business activities or processes are being designed or implemented
- existing processes are altered in a way that may alter the effectiveness of controls
- there has been a material change in the ACMA's operating environment
- 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

3.1.1 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.

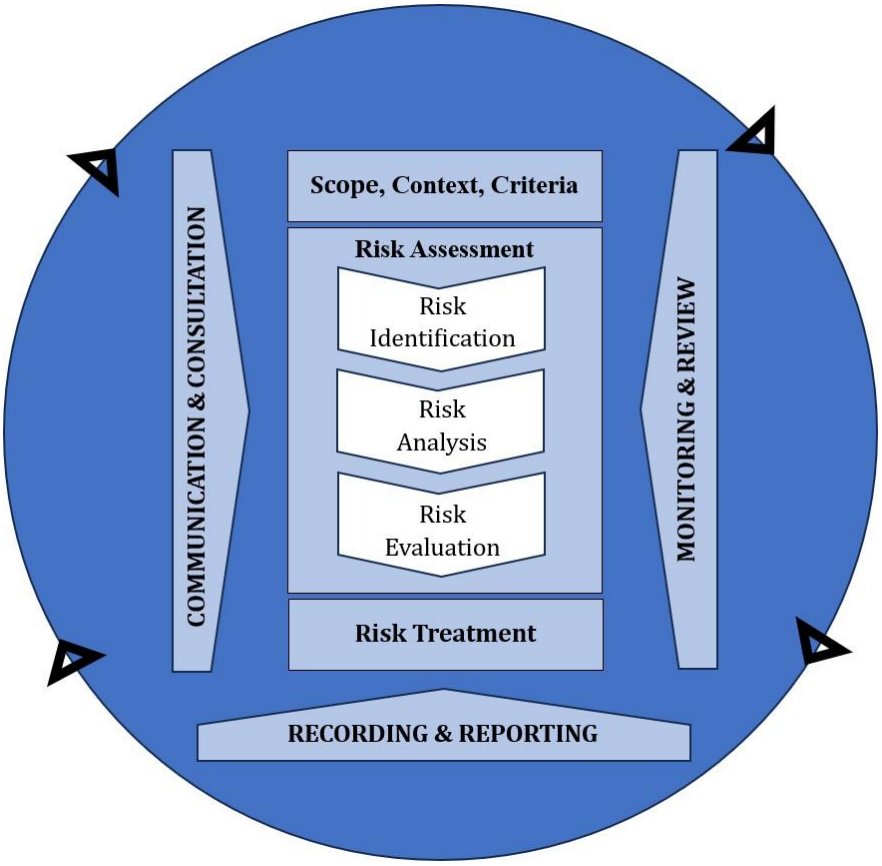


Figure 1: Risk Management Process

3.1.2 In addition, **Appendix A.1** of this Guide maps the risk management process against the Risk Management Plan template, to further assist officials make and record decisions.

3.2 Scope, Context and Criteria

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

3.2.2 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, including identifying any dependencies
- confirming who will be advised of the risk assessment, including which boards or committees (if any) will have oversight.

3.2.3 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.

3.2.4 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 Guide, 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

3.3.1 The purpose of a risk assessment is to establish an understanding of the level and nature of the risk, enabling the appropriate setting and the identification and prioritisation of controls and treatments. The risk assessment consists of the following steps:

- risk identification—finding, and describing the risk, the areas of uncertainty and the potential events that may affect the achievement of the objectives and determining the risk owner.
- risk analysis— assess the likelihood and consequence of the risk event occurring, taking into account the risk appetite, and the effectiveness of existing controls.
- risk evaluation—consider the risk analysis to determine whether additional actions (or treatments) are required and which risks are a priority.
- risk treatment—the action taken in response to the risk evaluation, where it has been agreed that controls in place are deemed ineffective and additional mitigation activities are required.

3.3.2 It is recommended that a risk assessment is conducted by at least two or three people working together, to allow for broader input. Senior leaders, risk and control owners should consult with operational staff when identifying and reviewing strategic, enterprise, divisional and discrete risks (including shared risks). Workshops or other meetings may

be used to help ensure all relevant perspectives are considered as part of the risk assessment.

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

3.3.4 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.

3.3.5 A summary of the process for conducting a risk assessment is available on The Hub, see Risk Assessment Fact Sheet.

3.4 Rating risks

3.4.1 The rating of risk is determined by considering the likelihood of a risk event occurring, the consequence of the event and the risk appetite that applies to the risk.

3.4.2 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.2**).

3.4.3 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.3**). 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.

3.4.4 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.4**). The rating associated with each level can be used in the ACMA risk register template to assist in the further consideration of risks.

3.4.5 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 guidance documents such as Standard Operating Procedures (SOPs).

3.4.6 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.

3.4.7 Risks are assessed and rated at three stages of the risk management process. See table below.

Inherent risk rating	Current risk rating	Target risk rating
The risk rating assessed without consideration of any existing controls or	The risk rating after considering the effectiveness of existing controls, representing the current level	The risk rating expected following the implementation of planned treatments,

treatments, reflecting the full effect of uncertainty on objectives based on inherent likelihood and consequence.	of risk based on adjusted likelihood and consequence.	representing the desired level of risk aligned with risk appetite and tolerance.

Table 1: Risk ratings

3.4.8 See the diagram in **Appendix A.5** to determine inherent, current and target risk.

3.5 Risk Identification

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

3.5.2 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?

3.5.3 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).

3.5.4 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 for each risk
- considering whether there are risks associated with conflicts of interest and the acceptance or provision of gifts, benefits, and hospitality.

3.5.5 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.

3.5.6 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.

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

- structured workshops
- environmental scanning
- Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis
- business process mapping
- analysis of complaints or past events
- scenario analysis
- obtaining expert advice
- audits or investigations.

3.5.8 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.

3.5.9 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.

3.5.10 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:

[Something that might occur] which leads to [consequences with reference to particular objectives] For example: *Physical security is breached by a malicious person which leads to the theft of ACMA equipment and repair and replacement costs.*

Table 2: General Approach to Describing Risk

3.5.11 The inherent risk should be rated and recorded in the relevant risk register template during the risk identification stage.

3.6 Risk Analysis

3.6.1 The purpose of risk analysis is to assess the likelihood and consequences of a risk event occurring, taking into account the risk appetite for that risk and the effectiveness of existing controls. This analysis will be used to determine the *current risk rating*.

3.6.2 During this stage, you should work with the control owner to identify the existing controls that are in place, classify the type of control and consider the effectiveness of controls. Further guidance about controls and control effectiveness, including control testing, is set out in the following sections 3.6 to 3.9 below and Chapter 6 of the Risk Management Policy.

3.6.3 The current risk should be rated and recorded in the relevant risk register during the risk analysis stage, after controls are in place.

3.7 Controls

3.7.1 A control is defined as 'any process, device, system, practice or other action that is put in place to regulate or modify the likelihood or consequence of a risk.' The main objective of implementing controls is to reduce the risk rating of a risk.

3.7.2 Control owners should formally document their controls in policy, processes and procedures and also record the control in the relevant risk register.

3.7.3 Controls should be classified into their types, depending on the aspect of the risk they control. A well-managed risk will have a spread of control types—preventative (p), detective (d), corrective (c). You should classify the control type in the risk register, typically by adding a (p), (d) or (c) after the control description. This can help to highlight where different control types may be needed to manage the risk.

3.7.4 Critical controls are those that are crucial to preventing the risk from happening or mitigating the consequences of the risk event. Even though other controls may exist, if a critical control were to fail, it would significantly increase either the likelihood or the consequence of the risk.

3.7.5 Questions to ask to determine if a control is critical include:

- Does the control represent a significant barrier to the risk event or prevent consequence severity?
- Is the control the only barrier or layer of protection preventing the risk event?
- Does the control prevent a number of threats or mitigate multiple consequences?
- Does the control operate independently to other controls?

3.8 Control effectiveness

3.8.1 A control's effectiveness should be assessed regularly to determine how well the control is managing the risk it has been designed to modify and to identify any gaps or deficiencies that need to be rectified.

3.8.2 A risk will have a range of controls that modify different aspects of the risk. Controls may work together to modify a risk, with some controls being more effective than others. The more effective a control is in its design and operation, the greater confidence there is that the associated risk is being managed effectively.

3.8.3 The ACMA takes a structured approach to assessing the effectiveness of controls through testing their design and operation. This provides assurance that the controls mitigate the associated risks to a level that is acceptable and consistent with the ACMA's risk appetite.

3.8.4 This approach should be applied to all controls in the ACMA's risk registers for strategic, enterprise, divisional and discrete level (project, program, section and business as usual [BAU) risk assessments.

3.9 Control testing

3.9.1 The purpose of testing controls is to:

- validate that controls are designed effectively
- confirm that controls are operating effectively
- identify gaps or weaknesses and recommend remediation.

3.9.2 Section 6.3 of the Risk Management Policy discusses the two main types of control testing—compliance testing and pressure testing—and the various methods for each type.

3.9.3 Compliance testing includes desktop review, system/process walkthrough or sample analysis. Pressure testing may be conducted on a periodic basis, with the approval of the relevant General Manager (GM).

3.9.4 A control(s) should be tested if the risk it is designed to manage is outside the ACMA's risk appetite statement and it:

- is a critical control(s) that plays a significant role in mitigating the risk;
- has failed to mitigate the risk; or
- has been recommended to PGAR for independent verification by the control owner, risk owner, the Audit and Risk Committee (ARC), or a governance committee, such as the Executive Management Committee (EMC) or the Enterprise Project Group (EPG).

3.9.5 Control owners may test specific controls or refer the testing to PGAR for independent verification or assurance.

3.9.6 PGAR will also coordinate a regular program of control testing, for independent verification or assurance. Under the program, a sample of controls will be selected for independent testing that would be conducted at least once every 12 months. The sample would include those referred by control owners. PGAR may conduct the testing or outsource it to the ACMA's internal auditor.

3.9.7 The results of a control's testing must be recorded in a Control Profile and Testing Form. The Control Profile and Testing Form is used to record details about each control and its testing results. The Control Profile and Testing Form template available through Microsoft Word ACMA shared templates and the Hub.

3.9.8 The Control Testing Guidelines (available on the Hub) set out the steps that should be followed when conducting control testing. The guidance applies to control owners, PGAR and the ACMA's internal auditor.

3.10 Risk Evaluation

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

3.10.2 Evaluation also involves 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.

3.10.3 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.6**). Regarding approval levels, the Chart specifies:

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

3.10.4 At the evaluation stage of a risk assessment, you should consider whether any risks need to be escalated. More information about risk escalation procedures is in section

3.11 below.

3.10.5 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.

3.11 Risk Escalation

3.11.1 Risk escalation is the process of referring risks to a more senior official, board or committee to consider implementing treatments or other actions that would modify the risk until it is at an acceptable level (see section 3.12 below). Risk escalation should occur promptly for timely decision-making and mitigation.

3.11.2 While risk owners have formal accountability for the escalation of their existing risks, all ACMA officials share responsibility for reporting risks that are outside our risk appetite and tolerance (section 5.3 of the Risk Management Policy).

3.11.3 Risks that are assessed as acceptable, that is, the risk rating is very low, low, or within our risk appetite, risk escalation is not required. Acceptable risks can be monitored or simply recorded in the relevant risk register.

3.11.4 As a starting point, the threshold for a risk being unacceptable and requiring escalation, is where the risk assessment has resulted in a risk rating of:

- high
- very high
- extreme
- outside our risk appetite.

3.11.5 Staff judgment may also be applied to assess if a low or medium-rated risk should be escalated, having regard to issues such as strategic significance, cross-entity impact and sensitivity.

3.11.6 Where a risk is assessed as unacceptable, the risk owner must consult promptly with stakeholders before escalating the risk. This will ensure that options and structured proposals to manage the risk are properly considered by all stakeholders.

3.11.7 When escalating a risk, the risk owner must escalate the risk to the appropriate senior official or governance committee, in accordance with the table below. Consideration should be given to the current risk rating, actions taken so far, recommended actions or decisions required and the urgency and timeframe for implementation. Please note, staff judgement may also be applied as to whether a lateral escalation (for example to a specialist function such as legal or cyber) may be appropriate.

3.11.8 The table below sets out the stakeholders and escalation reporting pathway for each type of risk.

Risk type	**Who is responsible for escalation**	**Stakeholders**	**Escalation**
Strategic	Risk owner	EM, Research Data and Governance branch RDG) PGAR Control/treatment owners	EMC Chair ARC
Enterprise	Risk owner	EM, RDG	EMC

		PGAR Control/treatment owners	Chair ARC National Work Health and Safety Committee (NWHSC)
Divisional	Risk owner	Relevant EM Control/treatment owners EPG NWHSC Relevant Authority lead Relevant Authority sub-committee	GM EPG NWHSC Chair EMC ARC
Shared risks with eSafety	ACMA and eSafety risk owners	ACMA and eSafety risk owners ACMA and eSafety control/treatment owners ACMA and eSafety Risk teams: PGAR and Governance Performance and Risk team ACMA and eSafety EMs/GMs	EMC (ACMA) SEB (eSafety) RCC (eSafety)
Discrete – Project	Risk owner	Relevant EM Relevant GM Control and treatment owners Project staff	EPG EMC Authority
Discrete – BAU	Risk owner	EM GM Relevant EL2 manager Control and treatment owners Line area staff	Stakeholder meeting

Table 3: Risk escalation reporting pathway

3.11.9 The diagram at **Appendix A.7** provides an overview of the risk assessment, escalation and treatment processes, and includes references to relevant sections of this Guide.

3.12 Risk Treatment

3.12.1 Risk treatment is the process to select and implement actions to modify an identified risk until that risk is assessed as acceptable. (See **Appendix A.7** diagram).

3.12.2 Treatment owners are responsible for implementing and monitoring treatments where the target risk level post control implementation is unacceptable.

3.12.3 Risk treatment is an iterative process as illustrated below:

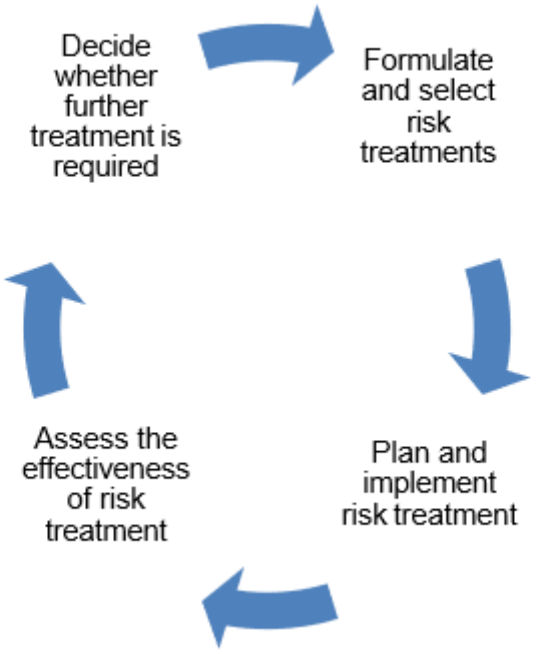


Figure 2: Risk Treatment Process

3.12.4 Treatments should be considered and agreed between all impacted stakeholders. The table in section 3.11.8 above lists the stakeholders who should be consulted for each type of risk. Each treatment should have a clear owner, outcomes and delivery timeframe. These aspects should be agreed at a key stakeholder or governance committee meeting. This is outlined in the diagram at **Appendix A.7**.

3.12.5 Formulating and selecting risk treatments involves balancing the proposed benefit of the treatment against the costs and resources required for its implementation. Treatments can be selected to remediate different aspects of the risk or control:

- Control enhancement—Treatment that modifies an existing control, such as closing out a weakness in a control or improves the control effectiveness.
- Compliance Gap—Treatment that aims to prevent a compliance breach or resolves a current compliance gap or breach.
- Risk Reduction—Treatment reduces the likelihood or consequence of the risk.

3.12.6 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).

3.12.7 In some cases, further treatment may be unachievable, or unaffordable, and the target

risk may need to be accepted and communicated.

3.12.8 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.

3.12.9 Agreed treatments should be recorded in the risk treatment section of the Risk Register template 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. If further treatments are required, they should be recorded in the Risk Treatment Plan and monitored until they are completed.

3.13 Treatment Evaluation

3.13.1 After each treatment is implemented, it is evaluated to determine if the risk has been reduced to an acceptable level (see **Appendix A.7**).

3.13.2 The evaluation is conducted by monitoring the treatment's implementation against the treatment plan and conducting a risk assessment to determine the target risk.

3.13.3 The key criteria for determining whether the treatment has been effective are:

- **Risk reduction—**how well the treatment has reduced the risk to an acceptable level, by reducing the likelihood and consequence of the risk and bringing it within our risk appetite and tolerance.
- **Timeliness—**how quickly the treatment has been implemented, whether it aligns with the urgency of the risk, the treatment plan timeline and the time to reduce the risk to an acceptable level.
- **Implementation completed—**the treatment was fully implemented, embedded in processes and adopted by stakeholder.
- **Strategic alignment—**whether the treatment's implementation aligns with organisational objectives and priorities and supports long-term goals and risk appetite.

3.13.4 Where appropriate, the following criteria can be also be considered when evaluating the effectiveness of treatments:

- **Value for money:** total cost of implementation (financial, time, resources); ongoing maintenance or operational cost; comparison of cost treatment versus cost of risk exposure; and return on investment.
- **Feasibility:** practicality of implementation within the current environment; availability of technology, resources, and skills; operational impact or disruption; and complexity and ease of execution.
- **Compliance and legal requirements**: alignment with laws, regulations, standards and policies; ability to meet audit or regulatory expectations; and avoidance of penalties or legal exposure.
- **Sustainability**: whether the control will remain effective over time; maintenance and monitoring requirements; and ability to adapt to changes.
- **Integration with existing controls:** compatibility with current systems/processes; avoiding duplication or conflict with existing controls; and ability to strengthen overall control environment
- **Risk interdependencies**: whether the treatment affects other risks (positively or

negatively); and potential to create new risks (e.g., outsourcing introduces third-party risk).

- **Measurability and monitoring**: ability to measure performance of the treatment with key performance indicators or control effectiveness metrics for ease of monitoring and reporting.

3.13.5 The risk should be reassessed, rated and recorded in the relevant risk register after treatments have been assessed.

3.13.6 If a risk treatment is assessed as acceptable, and therefore implemented in full, it is often considered to be a control. At that time, the implemented treatment can be removed as a treatment and added as a control in the risk register section of the Risk Management Plan.

3.13.7 If the risk treatment is assessed as unacceptable, then it must be escalated in accordance with section 3.11 and new treatments are generated and assessed until the risk is reduced to an acceptable level.

3.14 Recording and Reporting

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

3.14.2 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.

3.14.3 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.

3.14.4 Officials should refer to the Current Risk Level and Response chart in **Appendix A.6** for relevant approval levels for high, very high, and extreme risks.

3.15 Communication and Consultation

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

3.15.2 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.

3.15.3 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.

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

3.16 Monitoring and Review

3.16.1 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.

3.16.2 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.

3.16.3 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.

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

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

3.16.6 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.

3.16.7 The information gathered will inform the regular review of the Risk Management Framework.

Appendix A – Tables and Diagrams

A.1 Mapping the Risk Management Process against the Template

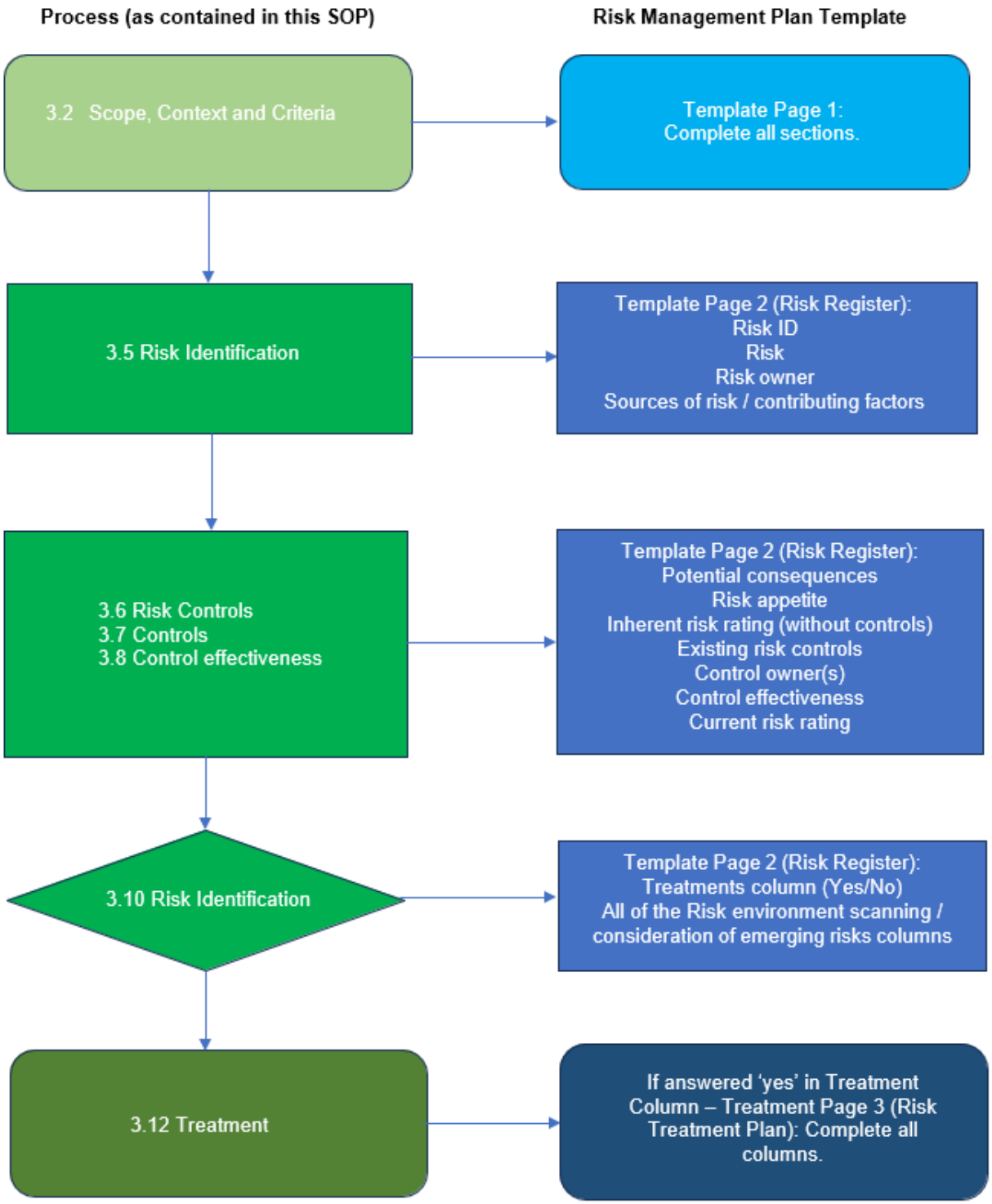


Diagram 1: Mapping the Risk Management Process Against the Template

A.2 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 4: ACMA likelihood table

A.3 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 5: ACMA consequence table

A.4 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 6: ACMA risk matrix

A.5 Inherent, Current and Residual or Target Risk

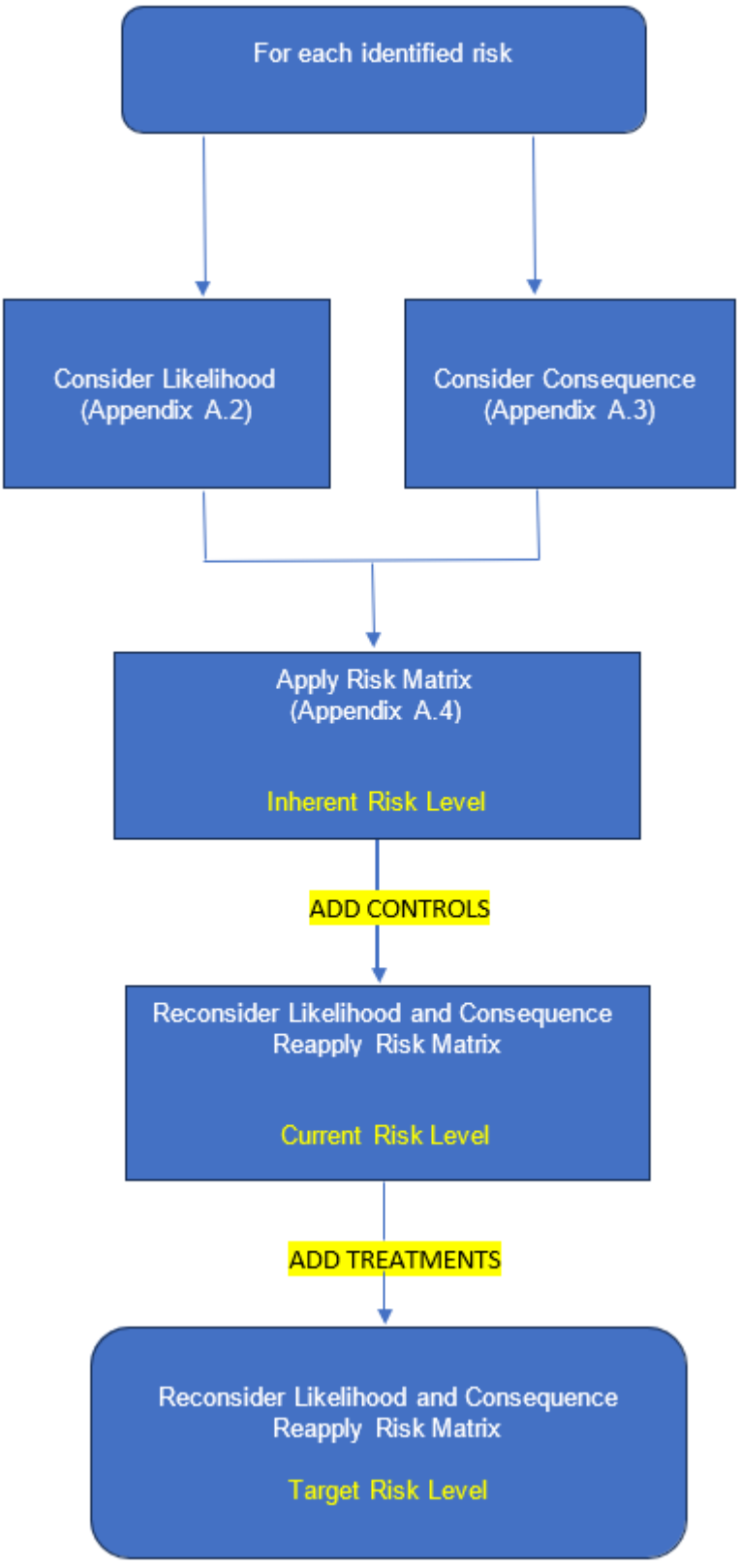


Diagram 2: Inherent, current, and residual or target risk

A.6 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 GM immediately. • In the absence of the GM, 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 GM 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 EM 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 7: ACMA risk levels and response

A.7 Risk assessment escalation and treatment diagram

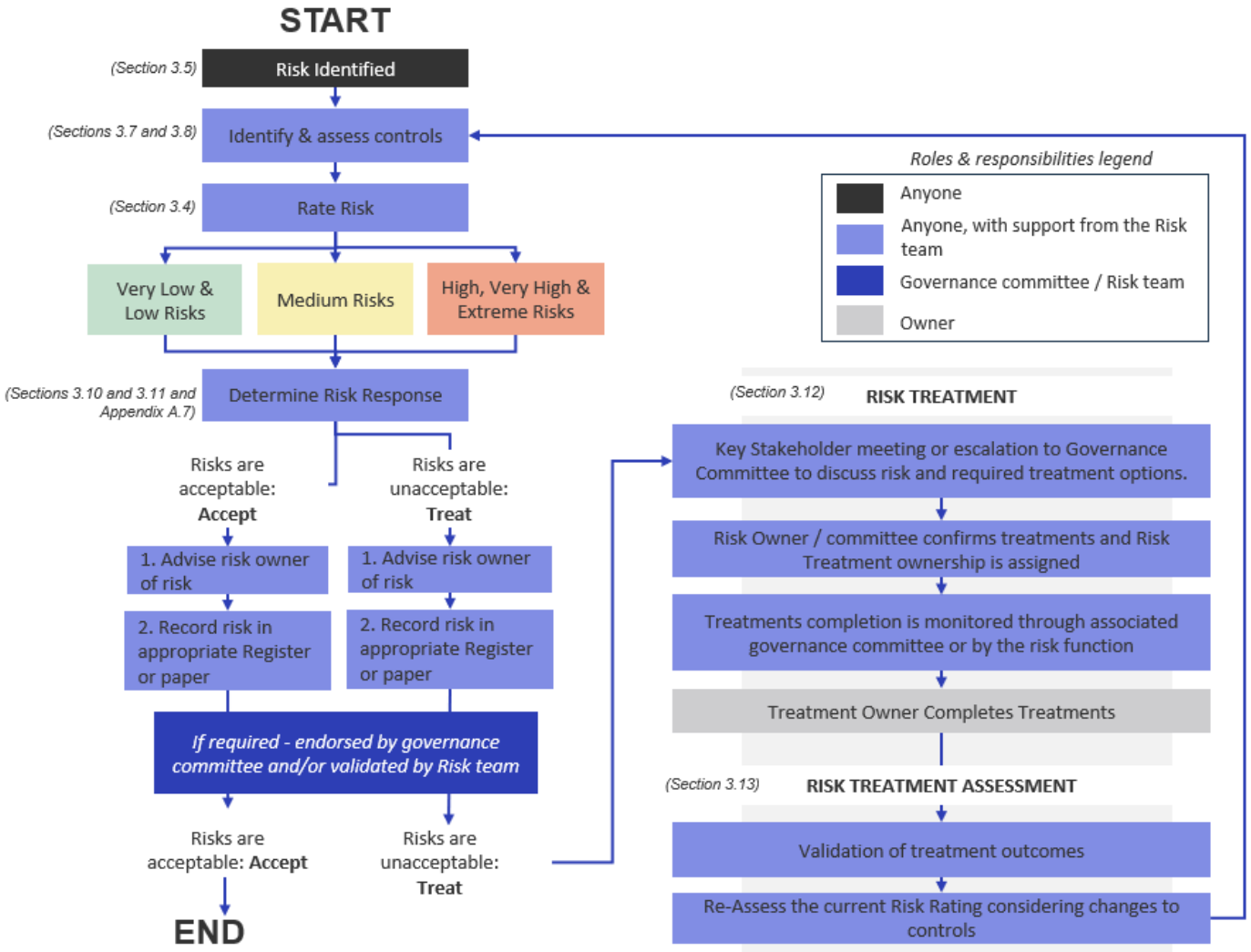


Diagram 3: Risk assessment escalation and treatment