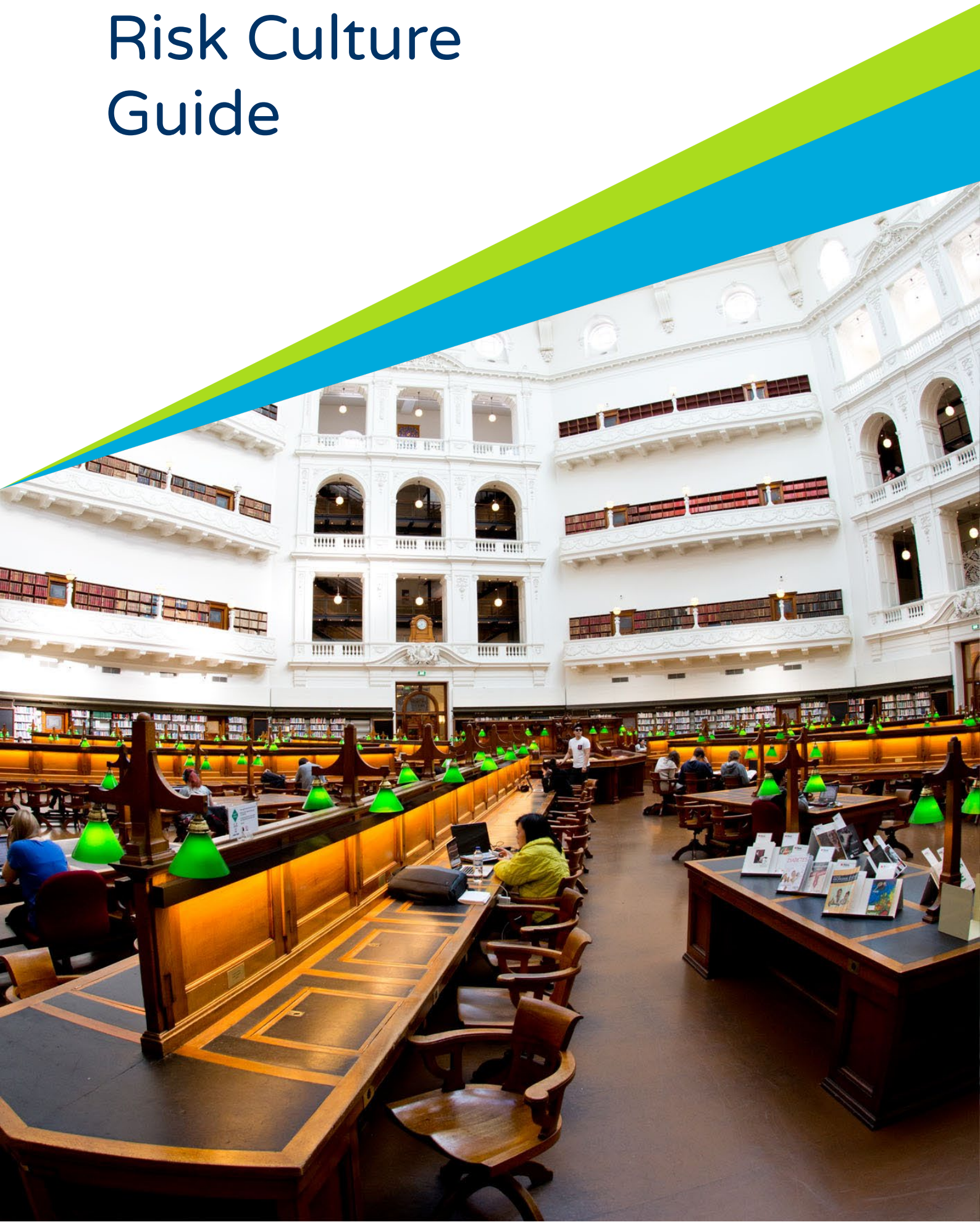
Risk Culture Guide



Contents

© Victorian Managed Insurance Authority

Level 10 South, 161 Collins Street Melbourne VIC 3000

PO Box 18409, Collins Street East Victoria 8003

ABN 39 682 497 841
P (03) 9270 6900
F (03) 9270 6949

contact@vmia.vic.gov.au

vmia.vic.gov.au

VMIA is the Victorian Government's insurer and risk adviser

Victorian Managed Insurance Authority (VMIA) acknowledges the Traditional Custodians of the land on which we do business and we pay our respects to Elders past, present and emerging. We acknowledge the important contribution that Aboriginal and Torres Strait Islander peoples make in creating a thriving Victoria.

Purpose

Effective risk management protects and creates value. It improves decision making, helps achieve your objectives and enhances overall performance.

Effective risk management is dependent on a positive 'risk culture'. Think about your organisation:

- How do people respond to risk management?
- Do they see it as a key part of their responsibilities?
- Is risk management seen as the Risk Manager's job and nobody else's?

The answers to these questions help identify a positive or negative risk culture.

Victorian government departments and public bodies covered by the Financial Management Act 1994 are required to support the development of a positive risk culture as part of the Victorian Government Risk Management Framework (VGRMF), and demonstrate the organisation's compliance with the framework. All other organisations are encouraged to adopt the VGRMF to enhance their risk management practices.

This guide offers practical support and guidance to meet the mandatory VGRMF requirements in relation to risk culture.

> You'll find this information more useful if you have an understanding of risk and the process of risk management. We have a range of resources to build your foundational risk knowledge.

What is risk culture?

Risk culture refers to the system of beliefs, values and behaviours throughout an organisation that shapes the collective approach to managing risk and making decisions.

Organisational culture and risk culture

Culture's the word used to describe the attitudes, beliefs, behaviours, and general norms of an organisation. Often, it's referred to as 'the way things are done around here'.

Each organisation has a different culture, and that's OK. An organisation's unique activities, operations and history means no two are the same. Sometimes, there are also different subcultures within an organisation, with varying accepted behaviours and norms.

Risk culture is related to organisational culture, but they aren't the same thing. Risk culture's the impact of organisational culture on how your organisation manages risk. Organisational culture is a key part of an organisation's risk management because it affects how people identify and manage risk. Improvements to risk culture can be difficult if there are underlying issues with overall organisational culture.

Aspects of Organisational Culture

What is a positive risk culture?

A positive risk culture is one where staff at every level appropriately manage risk as an intrinsic part of their day-to-day work.

People should value risk management and have an understanding and appreciation of the positive outcomes good risk management achieves. Staff should have the appropriate knowledge and skills, and be supported by internal processes and frameworks to help manage risk.

The word 'positive' is important, because the Victorian Government expects organisations to demonstrate positive risk behaviour. The opposite – negative risk behaviour – is likely to have adverse impacts for your organisation, government and the community.

The VGRMF (2025) asks organisations to consider some key principles when developing a positive risk culture. These principles are not compliance-focused, rather they provide a set of attributes to guide and assist in evaluating and improving risk culture.

Looking at your organisation's approach to these principles will highlight areas where you can demonstrate a positive risk culture:

Key Principles	Description
Tone from the top	Are your leaders at all levels living the organisation's values and displaying positive attitudes towards risk? Ensure you secure the buy-in and commitment of the leadership team and that they're leading by example.
Accountability	It's very important to clearly identify and communicate who is accountable for managing specific risks in your organisation and the responsibilities this entails. However, risk management is not solely the Risk Manager or Risk Owner's responsibility. All staff should be accountable for their actions around risk. Everyone needs to be clear about their decision-making responsibilities and when they should follow escalation procedures.
Strategy	Does your organisation have a clear strategy? Staff should understand how their work and responsibilities link to the organisation's strategy. It can also be difficult for individuals to influence the organisation's culture without a clearly articulated and endorsed strategy. A strategy will foster commitment from leaders and help develop an effective plan to improve your overall organisational and risk culture.
Communication	How are risks and the processes of risk management communicated across your organisation? Encouraging leaders to be transparent with their decision-making, and ensuring staff feel confident to 'speak up', helps everyone feel included and to take ownership in managing the organisation's risk.
Awareness and recognition of positive risk culture	Are all staff aware of what a positive risk culture is and what it looks like in your context? Developing strategies to recognise and reward positive risk behaviours can help raise awareness. Incentives can take the form of specific targets or KPIs, or you could design a 'Risk Champion' scheme to celebrate positive behaviours.

Escalation of bad news	Do staff members know how to escalate concerns and break 'bad news' to your leaders? Are people confident that they will not be penalised for calling out behaviours and questioning decisions? Escalation and challenge should be an opportunity for learning, rather than to blame individuals.
Supporting tools, templates and mechanisms	Does your organisation have the necessary resources to foster positive risk behaviours? Your organisation should have the relevant processes and tools to assist staff with risk knowledge, identification, assessment, escalation, and reporting. Some key mechanisms to consider are: • a clear and well communicated strategy that links to business unit's objectives and individual's responsibilities; • a risk management strategy, policy, and procedure; • a user-friendly and regularly reviewed risk register; • clearly articulated and communicated procedure for escalation that aligns with other policies and procedures, such as workplace health & safety, grievances, complaints & feedback and open disclosure; • a staff education or induction program.
Continuous improvement	Once your organisation has begun to evolve its risk culture, is there continuous monitoring and review? Organisational culture and risk culture are continually evolving and should be reassessed regularly, and improvement strategies realigned. Try to discourage a culture of complacency, and encourage behaviours that revolve around trust and challenge.

Practical Tip: Risk Champions

Enlisting Risk Champions across your organisation builds awareness and encourages recognition of the behaviours and attitudes needed to develop a positive risk culture. A Risk Champion is someone who supports the process of risk management and shares good practice across the organisation, or specifically within their individual teams.

Appointing Risk Champions does not mean recruiting new staff members. Instead, it means finding current staff who have an interest in supporting and promoting risk management. It's an opportunity for learning and development, and helps an organisation embed positive risk behaviours.

What is a poor risk culture?

There are many examples of poor risk culture leading to negative and harmful outcomes for an organisation's reputation and standing, with impacts spilling out into negative media coverage and impressions.

The 2019 Financial Services Royal Commission highlighted how a culture (and specifically, a risk culture) that prioritises financial gain above positive behaviours, risk-based decision making, and customer needs can lead to misconduct and poor outcomes. Many financial institutions were performing well financially, but profits were gained at the expense of their customer's financial stability, satisfaction, and in some cases, mental health.

When an organisation has a poor risk culture, negative workplace behaviours and decision-making often go unchecked. Many different behaviours and processes can be potential indicators of a negative risk culture, and often indicate that an organisation values short-term (usually financial) benefits over more long-term cultural improvements and value ethics.

Often, this leads to a lack of transparency and reporting, lack of accountability, and infrequent and ad hoc communication and decision-making. Decision-making that does not consider all risks and potential effects on people harms everyone, including customers, staff, the wider community, and an organisation's reputation.

Look out for risk culture 'red flags'

Just as there are indicators that an organisation is demonstrating a positive risk culture, there can be signs that an organisation's risk culture is poor. Some examples of risk culture red flags may include:

- Staff not feeling empowered to raise concerns to leaders and fear reprisal
- Risk management is considered a compliance issue only
- Decision-making is ad hoc, and staff rarely understand why certain decisions have been made
- Staff do not understand how their roles and responsibilities relate to the organisation's overall strategy
- There is no risk management strategy or framework
- Lack of robust recruitment and screening processes
- High staff turnover
- Low customer or service user satisfaction.

How do I build a positive risk culture?

Building a positive risk culture requires ongoing commitment and continuous improvement. This will ensure people have the opportunity to grow and improve their risk management capability and adjust behaviours over time.

As every organisation is different, there is no 'one size fits all' approach to building a positive risk culture. There are many definitions and methods that can be used. The VGRMF describes the process of building a positive risk culture in three key steps:

- Understanding the organisation's current risk culture and defining the desired risk culture;
- Identifying any gaps between the organisation's current risk culture and desired risk culture; and
- Defining the organisation's approach to evolve the organisation's risk culture to close gaps over time.

Whilst evolving culture is a gradual process, organisations can break down these steps into smaller, more practical actions to help build a positive risk culture.

Step 1: Understanding

Understand your organisation's current risk culture

Before you can build your positive risk culture, it's important to understand your organisation's current risk culture. This means examining certain parts of your organisation's culture and assessing how well they support your organisation's approach to managing risk.

Measuring risk culture, and culture more generally, can seem like an overwhelming task. One way to make it manageable is to divide risk culture into more easily measurable attributes. Looking at your organisation's current attitudes to risk management along with other aspects of your broader organisational culture, such as operational processes, capability, relationships, and values, will help to identify positive cultural aspects to build on and areas that may need improvement.

A quick way to start the conversation around measuring your risk culture is to use the Risk Culture Health Check Tool on the next page of this guide. These questions will help assess how your organisation performs across a range of positive risk culture behaviours and practices, and may highlight areas for further assessment or improvement.

Risk Culture Health Check

This simple health check has been designed to help begin an assessment of your organisation's risk culture. The questions will test perceptions about attitudes to the management of risk, or risk culture, in your organisation. They have been designed to reflect the key principles of a positive risk culture outlined in the VGRMF.

Try to think about how people at all levels of your organisation might respond to these statements. Or, ask a range of people to complete the tool and collate their feedback. Try to be as honest as possible in your scoring.

	Strongly disagree				Strongly agree	Don't know
Select one answer for each statement.	1	2	3	4	5	
Tone of the organisation						
Our leaders at every level act and behave in ways that clearly show managing risks is very important.	☐	☐	☐	☐	☐	☐
Poor behaviours (such as bullying, favouritism and ignoring conflicts of interest) are not tolerated in this organisation.	☐	☐	☐	☐	☐	☐
Accountability						
Our leaders at all levels challenge people constructively and positively if they do not meet their commitments to manage risks.	☐	☐	☐	☐	☐	☐
Strategy						
We have a clear strategy for building and sustaining a positive risk culture and this is being executed successfully.	☐	☐	☐	☐	☐	☐

Communication	
People are comfortable in sharing ideas and speaking up about how to manage risks more effectively.	☐ ☐ ☐ ☐ ☐ ☐
Awareness and recognition of positive risk culture	
Our leaders regularly and effectively communicate about the importance of each person taking responsibility for managing risks in their role.	☐ ☐ ☐ ☐ ☐ ☐
The way our people behave shows that each person believes they have a responsibility for managing risks in their own role.	☐ ☐ ☐ ☐ ☐ ☐
Escalation of bad news	
Most people in our organisation, if they identify risks that have not been properly managed, are comfortable informing their manager or other senior executives.	☐ ☐ ☐ ☐ ☐ ☐
Supporting tools, templates and mechanisms	
We are provided with good tools to help manage risks, and we are well trained in how to use these.	☐ ☐ ☐ ☐ ☐ ☐
Continuous improvement	
In our organisation we are constantly searching for ways to strengthen and improve our risk culture.	☐ ☐ ☐ ☐ ☐ ☐

Developed with thanks to Dawson McDonald Consulting.

In addition to this healthcheck you can use other methods to assess risk culture:

Risk Maturity Benchmark	A more in-depth self-assessment of your approach to managing risk can be done using VMIA's risk maturity assessment tool, the Risk Maturity Benchmark (RMB). The RMB's available to Victorian government departments and public bodies covered by the Financial Management Act 1994.
Surveys	Staff surveys can provide more detail and insights into your current risk culture. You might decide to survey a percentage of staff across the organisation or include some questions around risk management knowledge and behaviours in one of your existing staff surveys. You may choose to include some questions from the Risk Culture Health Check Tool.
Audits & Interviews	Your organisation may also want to do peer-to-peer or third-party interviews to validate your self-assessment or survey data. Self-assessment and surveys alone can suffer from subjectivity. Interviews conducted by peers or third parties can provide a safe environment to discuss feelings and attitudes toward risk without concerns about how leaders may perceive responses.

Articulate the desired risk culture

Once you understand your current risk culture, your organisation decide on its desired future state. When doing this, think about what's appropriate and achievable for your organisation's activities and needs.

Changing even just one element of your culture will require time and effort. When setting yourself targets, it's important to consider a staged approach. Think about:

- What can your organisation realistically aim for this year?
- What should be completed in future years?
- What are reasonable short, medium and long-term targets?
- Does your desired risk culture take your vision, values, and strategic objectives into consideration?

Practical Tip: Stop, Start, Continue

It can be difficult to describe your organisation's desired culture. Instead, consider describing 'desired behaviour'. Having clear instruction about which behaviours to "Stop. Start. Continue." can be a quick way to identify behaviours that encourage positive risk culture.

Work to articulate and consistently communicate these across your organisation:

- What should you stop doing?
- What should you start doing?
- What should you continue to do?

Step 2: Identifying

Identify any gaps

Once you've articulated your desired risk culture, identify where there are gaps from your current state assessment. When identifying gaps, consider:

- Are there any quick wins that can be implemented in the first stage of a risk culture action plan?
- Where are the major gaps?
- Should any gaps be captured in the risk register for specific action and monitoring?
- Where will your organisation need to develop a long-term, staged approach to sustainably bridge the gaps?

Gaps identified between the current and desired state should be reported to the relevant governance committee and leadership. Any gaps and quick wins can form the basis of your approach to evolving your organisation's risk culture.

Step 3: Defining

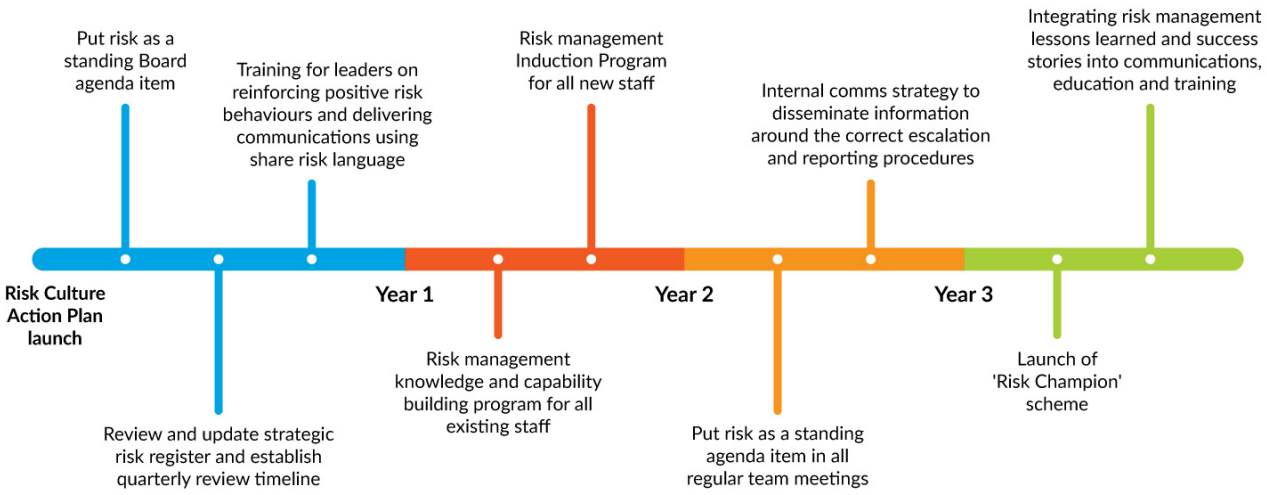
Define the organisation's approach to evolve the organisation's risk culture

Once the desired risk culture is articulated and gaps identified, develop an action plan to evolve your organisation's risk culture. The scale and complexity of your action plan should reflect your organisation's size and activities.

A risk culture action plan should be outlined in your risk management strategy. It should consider other risk management activities (such as your broader risk management framework, how risk is communicated, and risk reporting timelines) but keep focus on the **cultural aspects** of risk management. It's also a good idea to work alongside human resources and communications staff, to confirm an approach that is aligned to other organisational activities and goals.

A risk culture action plan should consider:	
Prioritisation	Which improvement opportunities can commence immediately, and which ones will need to be gradually developed over time? How much value will each opportunity add to the organisation, and how difficult it will be to implement?
Accountability	Who is accountable for each improvement opportunity? While risk is everybody's responsibility, each improvement opportunity should be assigned to a staff member, who will be responsible for ensuring its successful implementation.
Embedding	How will your organisation make sure that the desired behaviours, values, and capabilities become an accepted part of the way the organisation operates? Culture cannot be changed by creating rules and procedures alone. Focusing on small but consistent changes to behaviours and attitudes around risk can be a good step to demonstrating a positive risk culture.

Risk culture road map example, Figure 3



Practical tip: Test your action plan

Instead of rolling out your action plan across the entire organisation at once, test it in one unit or division. Use this to get feedback from people on the front line about what works well and what needs to change. Use this feedback constructively to improve your action plan before launching it across the organisation.

Step 4: Continuous Improvement

Monitor, Reporting, and Review

Monitoring the implementation of your risk culture action plan is essential to demonstrate its success. Circumstances are likely to change during a long-term, staged approach, so periodic review should occur alongside any monitoring of individual improvement opportunities.

Reporting should be defined in the action plan and aligned to the agreed risk management reporting cycle. The Accountable Officer, relevant risk governance committees, executive and leaders should be regularly informed of progress and setbacks that might occur along the way.

Refine plan

Developing a positive risk culture takes time. The action plan and overall risk management strategy should be refined over time to ensure they continue to reflect the organisation's expectations and align to the vision, values, and objectives for risk management