Risk Management

The aim of Insights: Audit Lessons is to communicate lessons from our audit work and to make it easier for people working within the Australian public sector to apply those lessons.

This edition of Insights: Audit Lessons is targeted at risk practitioners and officials responsible for government operations, projects, programs, services and regulatory activities. It would also be useful for accountable authorities, their senior executives and audit and risk committees.

Commonwealth Risk Management Policy

The Commonwealth Risk Management Policy, first established in 2014, aims 'to embed risk management into the culture and work practices of [Australian Government] entities to improve decision making in order to maximise opportunities and better manage uncertainty'. The policy was updated in November 2022.

The policy supports section 16 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), which states that 'the accountable authority of a Commonwealth entity must establish and maintain an appropriate system of risk oversight, management and internal control for the entity'. The policy has nine elements.

Risk management findings in ANAO audits

ANAO audits regularly assess risk management practices in Australian Government entities and often find that entities are not appropriately managing risk by meeting all elements of the Commonwealth Risk Management Policy.

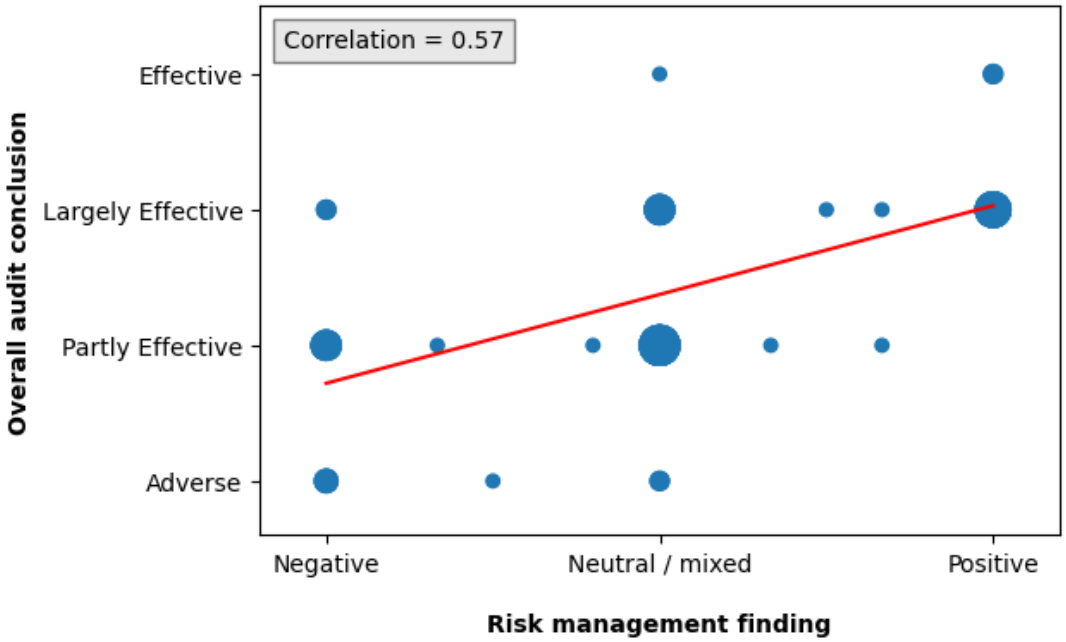
Note a: For this analysis, audits were considered to have examined risk management if either the audit objective, criteria or sub-criteria explicitly included an assessment of risk, or if there was a discussion of risk management practices as part of a broader sub-criterion, for example a sub-criterion relating to governance arrangements.

Note b: In this context, 'audit findings' refer to results against audit sub-criteria. These are presented in grey boxes in audit reports.

Note c: The summary and recommendations chapter of each performance audit report includes key messages from the audit for all Australian Government entities.

In ANAO audits tabled between July 2021 and June 2023, there is a positive relationship (+.57) between risk management findings in the audit and the overall audit conclusion (see Figure 1). In other words, if an audit has positive findings about risk management, more likely than not, the overall audit conclusion will be positive.

Figure 1: Relationship between risk management findings and overall audit conclusions



Note: One data point (dot) in the figure may represent more than one audit if multiple audits had the same result. There were 40 audits assessed for this correlation analysis. These equate to 16 dots in this figure. The larger the dots, the more audits represented by that particular dot.

Lessons on risk management

This edition of Audit Lessons sets out eight lessons aimed at improving risk management practices, based on ANAO audits over five years (July 2018 to June 2022).

The ANAO Insights publications listed under further reading provide additional lessons for managing risks in specific contexts, such as fraud control or in emergencies.

The Department of Finance provides resources (see Risk Management Services) to support entities with risk management.

1. Put the fundamentals in place

Putting in place the fundamentals is necessary for good risk management. The fundamentals include:

- a formalised approach to risk management in a risk management framework (Element Two); and
- arrangements to operationalise risk management frameworks such as supporting policies and procedures.

An entity's risk management framework should set out how it will meet the Commonwealth Risk Management Policy. For example, it should clearly define the responsibilities for managing risk within an entity (Element Four) and indicate how an appropriate level of risk management capability will be maintained (Element Eight).

Appropriately documenting an entity's approach to risk management is a prerequisite for effective risk management. Documentation that supports systematic and consistent risk management gives stakeholders visibility and supports transparency and accountability.

The following indicate that the fundamentals of good risk management are in place.

Case study 1. System of risk oversight and management — Northern Land Council

The ANAO completed an audit of the Northern Land Council's (NLC) governance arrangements in August 2023. The audit found that the NLC had a risk management framework. The framework set out governance arrangements and a process for managing risks. It included tools, guidance and training for personnel. The framework also set out monitoring and reporting arrangements.

Although these elements were in place, the audit identified that the effectiveness of the framework as undermined by the following issues:

- the framework was in draft, although personnel had been instructed to comply with it;
- while the NLC maintained a risk register, the register did not articulate whether assessed risks exceeded the risk appetite and did not always record information to demonstrate that risks had been reviewed each quarter;
- risk management training was not mandatory (between November 2020 and November 2022, seven per cent of permanent personnel completed the training); and
- quarterly risk reporting was not undertaken, as planned, reducing oversight.

To read more, see paragraphs 4.1 to 4.11 of *Governance of the Northern Land Council*.

2. Create a positive risk culture

Creating a positive risk culture is not a standalone activity, it is created through actions on a variety of fronts.

A positive risk culture is essential to effective risk management, which in turn is essential for organisational success.

An entity's risk management framework must support a culture where risk is managed and communicated across all levels of the entity and individuals are encouraged to adopt positive risk behaviours (Element Three). The culture should encourage bad news to be escalated, without fear of reprisal.

An entity's risk management framework should set out its approach to promoting a positive risk culture.

An August 2018 paper from the Auditor-General — Strategic governance of risk: Lessons learnt from public sector audit — provides additional information about creating a positive risk culture.

The following are typical characteristics of an entity that has a positive risk culture.

Case study 2. Creating a culture of cyber resilience to manage cyber security risks

Although the following audit focussed on the cyber security risk culture, the audit findings are also relevant to creating a broader positive risk culture.

In the audit *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*, the ANAO examined whether selected entities had established strong cyber resilience cultures to assist in managing cyber security risks.

In creating a cyber resilient culture, the three examined entities had undertaken the following.

- *Established clear responsibilities for senior leaders* — a responsibility of all senior leaders and governance bodies was to be aware of cyber vulnerabilities and threats.
- *Defined and communicated risk management roles and responsibilities* — information security roles were assigned to relevant staff and respective responsibilities were communicated; and the entities ensured management representatives understood their roles and responsibilities.
- *Communicated about risk management* — security awareness was embedded as part of the enterprise culture, including expected behaviours in the event of a cyber incident.

- *Followed through on commitments* — there was an approach to verify the accuracy of self-assessments of compliance with cyber security requirements; and documented investment plans for the current budgets and projects.

To further embed a cyber resilient culture, the entities could have done the following.

- *Increased training opportunities for staff* — by developing the capabilities of ICT operational staff to ensure they understood the vulnerabilities and cyber threats.
- *Better integrated risk management into operations* — by:
  - adopting a risk-based approaches to prioritise improvements to cyber security and to ensure higher-risk vulnerabilities were assessed;
  - developing and implementing an integrated and documented architecture for data, systems and security controls; and
  - identifying and analysing security risks to information systems.

To read more, see paragraphs 4.1 to 4.18 of *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*.

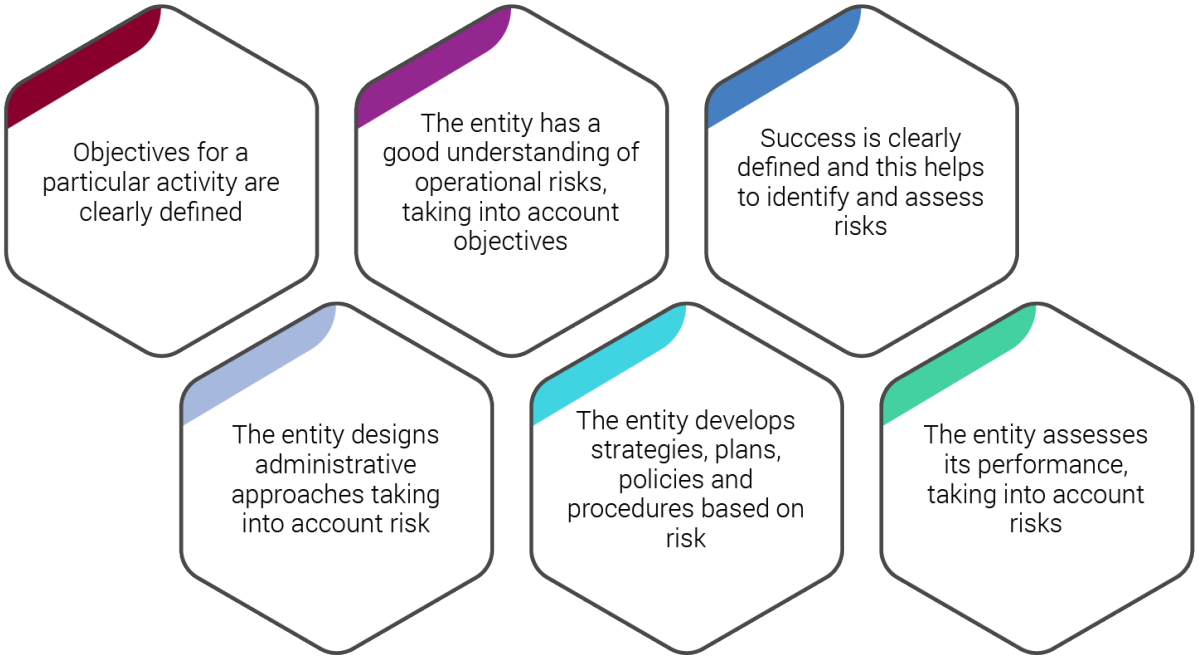
3. Tailor administration based on risk

Everything involves risk to varying degrees — risk management should be a feature of all government activity and be fit for purpose.

Risk is the effect of uncertainty on the achievement of objectives, whether positive or negative. To tailor administration based on assessed risk, entities should consider the following.

- Developing a good understanding of strategic and organisational risks involves determining what information is needed and how it will be collected.
- Risk management practices should be proportionate to the level of risk and the scale of a particular activity.
- The administrative approach for an activity (e.g. the process for conducting a procurement) should be designed and adapted based on risk.
- Performance frameworks should be informed by risks. As an example, in a regulatory context an entity may establish a risk-based compliance program. Performance frameworks should assess whether the entity has effectively addressed compliance risks through its compliance program.

The following indicate that administration is being tailored based on risk.



Case study 3. Revenue collection — the Australian Taxation Office's (ATO's) tax gap program

In *Identifying and Reducing the Tax Gap for Individuals Not in Business*, the ANAO examined the ATO's tax gap program for the individuals not in business market.

Through its tax gap program, the ATO estimates the difference between the amount of tax it collects and what it would have collected if every taxpayer was fully compliant with the law. This measure gives the ATO an understanding of risk (of non-compliance). In the individuals not in business markets, the gross tax gap was six per cent — that is, revenue collection was estimated to be six per cent lower than if all taxpayers were fully compliant.

The ATO's uses its understanding of tax gaps in the various markets to inform the identification and assessment of business and enterprise-level risks and the development of risk-based compliance strategies.

The ANAO recommended that the ATO could set specific measurable targets and develop benchmarks to measure and evaluate its activities. This would assist with assessing the impact of its compliance strategies in addressing the risk of non-compliance.

To read more, see *Identifying and Reducing the Tax Gap for Individuals Not in Business*, particularly Chapter 3.

4. Embed risk management into decision making

Decision makers should be provided with the appropriate quality and quantity of risk information to make informed decisions.

Risk management must be embedded into decision making (Element One). This works best when risk management is an integrated or part of decision-making processes. Decision makers should request more information about risks, if they require it.

The following indicate that risk management is embedded into decision making.

Case study 4. Assessment of policy option risks — temporary expansion of COVID-19 telehealth services

Telehealth services refer to real-time clinical consultations conducted via video conferencing or phone rather than face-to-face. In *Expansion of Telehealth Services*, the ANAO found that the Department of Health and Aged Care (Health) advised the Minister for Health on the costs of telehealth in the context of COVID-19, but only some of the benefits and risks. This impacted the decision maker's ability to make fully informed decisions about expanding telehealth services.

Between February and May 2020, briefings and discussions between Health and the Minister for Health included only some consideration of risks in relation to the temporary expansion of telehealth services.

- For policy proposals valued at over $30 million, risks should be assessed using a risk potential assessment tool. This tool is used to provide a standardised assessment and presentation of risks in policy proposals. Health did not assess the risks of the COVID-19 telehealth temporary policy options between March 2020 and May 2021 in accordance with this requirement.

- Between June 2020 and August 2021, discussions were held between Health and the minister on options to make telehealth permanent. Risk potential assessment tools were used for these policy options, in accordance with requirements.

To read more, see paragraphs 2.8 to 2.26 of *Expansion of Telehealth Services*.

5. Establish fit-for-purpose risk controls and treatments

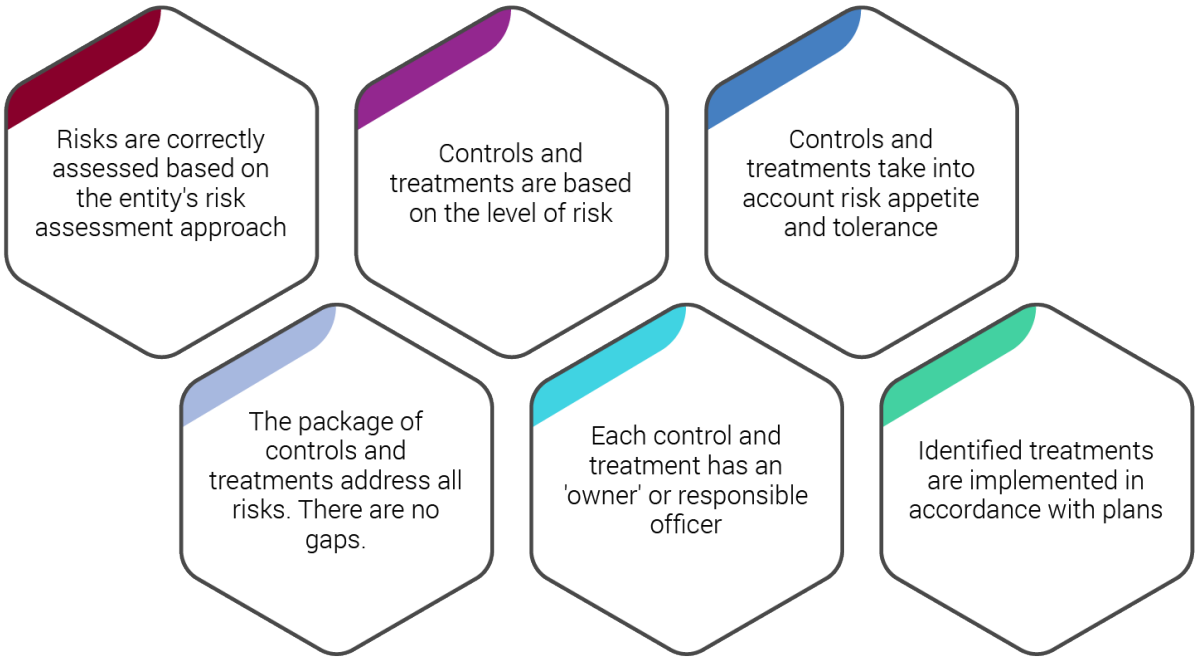
Having a systematic approach to identifying, implementing and monitoring the effectiveness of controls and treatments increases the chances of success.

Risks are ultimately managed through controls and treatments.

- The success of managing risks relies on the effectiveness of controls and these controls being monitored. Controls can be preventative, detective and corrective. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk (ISO 31000: 2018 Risk Management).
- If controls are insufficient, then treatments or mitigations should be developed to lower the risk to an acceptable level. Once treatments are implemented, they become controls.

Controls should be regularly reviewed to ensure that they are effective. Action should be taken if they are not working as intended — see Lesson 8.

The following indicate that there are fit-for-purpose controls and treatments to manage risks.



Case study 5. Assessing and treating Superannuation Guarantee Charge risks

In the audit *Addressing Superannuation Guarantee Non-Compliance* the ANAO found that the Australian Taxation Office (ATO) had not appropriately assessed the consequence of a relevant enterprise risk, which led to a lower than merited risk rating.

This in turn meant that the ATO had not established adequate controls and treatments to manage this risk. The relevant enterprise risk was 'that employers fail to report and pay their SG [Superannuation Guarantee] contributions correctly and then fail to lodge and pay the resulting Superannuation Guarantee Charge'. The ATO rated this risk as 'significant', however, it did not take into account the revenue at risk represented by non-compliance with Superannuation Guarantee Charge requirements.

Had the ATO factored revenue at risk into its assessment of this risk, the risk would have been rated as 'high' rather than 'significant', which had follow-on consequences for how the risk should have been escalated and treated.

To read more, see paragraphs 2.16 to 2.31 of *Addressing Superannuation Guarantee Non-Compliance*.

6. Keep a watch out for emerging risks

Risk management is not a static exercise. The more an entity's operating environment is subject to change, the greater the need for robust processes to identify and manage emerging risks.

Emerging risks are newly developing or evolving risks that can affect the achievement of an organisation's objectives.

Entities must establish arrangements for identifying, managing and escalating emerging risks (Element Seven). Risk management plans must be periodically reviewed and updated.

The following indicate that emerging risks are being identified and managed.

Case study 6. Assessing emerging risks during the COVID-19 vaccine rollout

In *Australia's COVID-19 Vaccine Rollout*, the ANAO examined the Department of Health and Aged Care's planning and implementation of the COVID-19 vaccine rollout. The audit noted that the department was aware 'that vaccination of the entire Australian population would be attended by many risks' and that these risks would change over time. For example, initially it was not known whether a COVID-19 vaccine would even be developed. When it became clear that vaccines would likely be available, risk management became more focused on the rollout of a vaccine.

The audit found that the department had robust arrangements in place to identify and assess emerging risks to the rollout. The department:

- established a comprehensive risks and issues register which was used throughout 2021 to identify risks to the rollout;
- kept risks under regular review — this included 'deep dives' for the top risks and issues; and
- determined corrective action, where necessary.

The most significant risks and issues were referred to the rollout taskforce for review.

The audit found that 'the consistent use of a risk register and a documented process to respond to risks as they arose demonstrates good practice'.

To read more, see paragraphs 2.38 to 2.47 of *Australia's COVID-19 Vaccine Rollout*.

7. Consider additional factors for shared risks

Managing shared risks requires additional consideration because different parties are likely to have different objectives, different perceptions of risk and different risk management approaches. ANAO audits find that the management of shared risks is a particular area of weakness.

The Department of Finance outlines that shared risks have some distinguishing features. They may not have an obvious 'owner', may be more complex in nature because they might be influenced by multiple parties and, if they are realised, can impact different organisations in different ways.

Entities must collaborate to manage shared risks (Element Six). It is important that there are mechanisms in place to develop a common understanding of shared risks and to set out the structures to manage those risks. Entities may also have different enterprise approaches to managing risks. For shared risks, there may need to be a compromise in establishing a common approach that is fit-for-purpose to managing the shared risks.

The following indicate that shared risks are being effectively managed.

Case study 7. Managing shared risks relating to the accuracy and timeliness of welfare payments

In *Accuracy and Timeliness of Welfare Payments*, the ANAO found that the Department of Social Services (DSS) and Services Australia did not have mechanisms to support the proactive and strategic management of shared risks relating to payment accuracy and timeliness.

- There were five bilateral service arrangements relating to payment accuracy and timeliness. Only one of these included references to risk management.
- DSS developed payment accuracy risk management plans, however, these plans were not shared with bilateral governance bodies.
- Although both DSS and Services Australia had policies for managing shared risks, these were not always followed. DSS and Services Australia had not developed joint risk management plans or shared risk registers. Engagement at bilateral governance bodies focussed on managing emerging issues, rather than proactive and strategic discussion of shared risks.

The audit recommended that DSS and Services Australia implement robust bilateral processes to manage shared risks. This included establishing and maintaining joint risk management plans and/or registers.

To read more, see paragraphs 2.42 to 2.56 of *Accuracy and Timeliness of Welfare Payments*.

The audit — *Implementation and Performance of the Cashless Debit Card Trial — Follow-on* — also provides an example of the management of shared risks. See paragraphs 2.18 to 2.21.

In January 2022, the ANAO published *Service Delivery through Other Entities*. In section 2 of this Insights publication, there is a discussion and further examples of managing service delivery risks between multiple agencies.

8. Continually monitor and review

Do not assume that everything is working as intended — there needs to be continual monitoring and review of an entity's approach to how risk is managed including the effectiveness of controls and risk treatments.

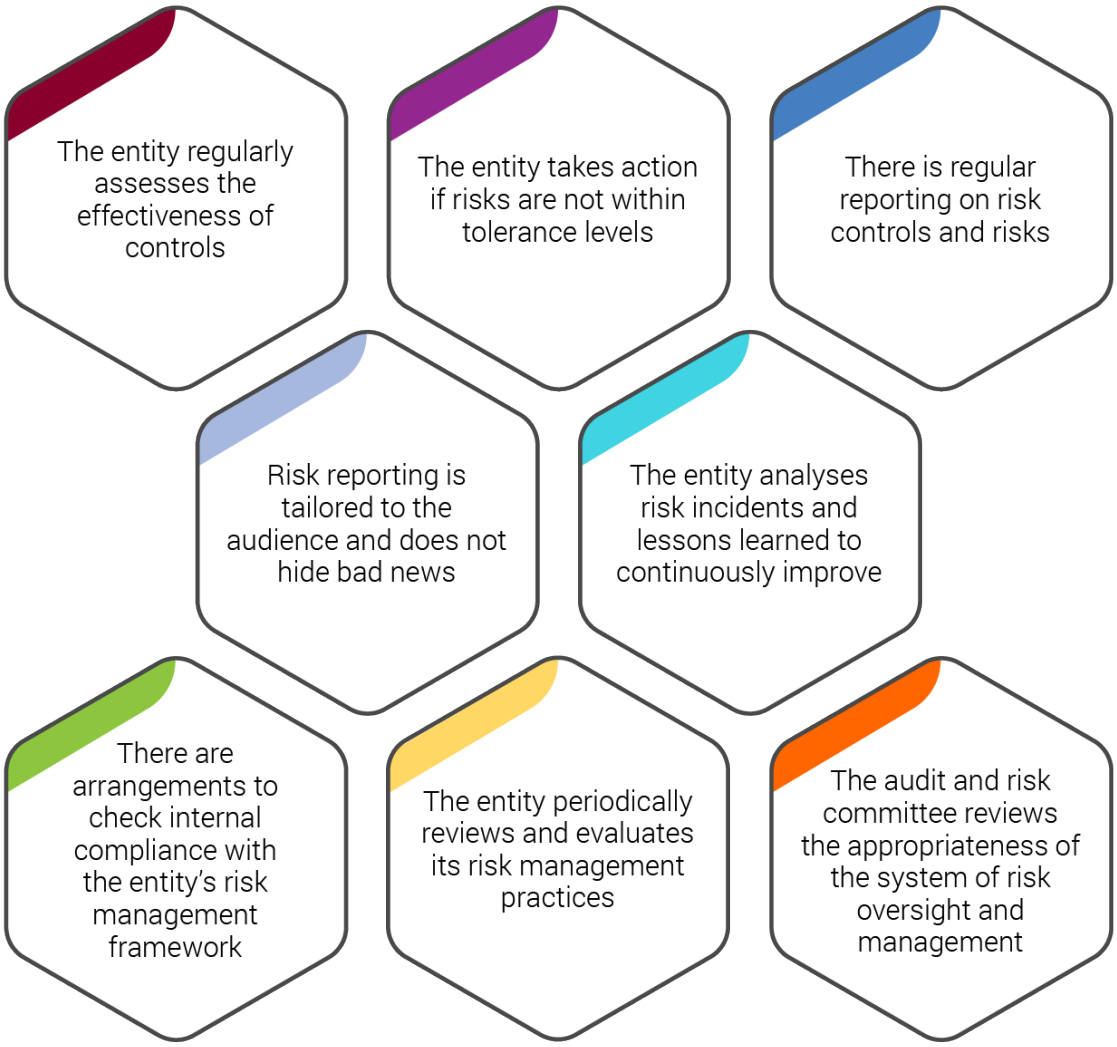
Entities must assess the effectiveness of controls to manage risks (Element Five) and regularly review their approach to managing risk (Element Nine).

Risk management is most effective when risks that are outside the documented risk tolerance levels are identified and treated. This means that there should be ongoing monitoring of risks and associated controls. If risks are not within tolerance levels, prompt action should be taken.

Regular, simple, clear and complete reporting on risks should be suited to the intended audience. Reports should not attempt to hide bad news.

Entities should also periodically step back to evaluate whether their risk management practices are effective with a view to continuous improvement.

The following indicate that risk monitoring, reporting and review arrangements are fit for purpose.



Case study 8. Assessing controls for managing risks to material misstatements in financial statements

For financial statements audits, the ANAO seeks to gain assurance that an entity has an effective internal control framework to manage the risk of material misstatement.

Entities undertake a range of activities to monitor and assess their internal controls. These activities include external reviews, self-assessment processes, post-implementation reviews and internal audits. The nature and extent of these activities should be informed by risk. The ANAO applies a risk-based approach to determine its review of these activities.

There is also a structured compliance reporting process for financial statements, which requires that entities report on significant non-compliance. This includes reporting on systemic issues reflecting internal control failures or high-volume instances of non-compliance.

The preparation of financial statements is mature and ongoing and, as such, practices for assessing internal controls and reporting are well established.

To read more, see paragraphs 1.10 to 1.27 of *Interim Report on Key Financial Controls of Major Entities* (25 May 2023).

Further reading

Insights: Audit Lessons

- 21 November 2017 — Corporate Planning, Performance Statements and Risk Management under the PGPA Act.
- 17 May 2019 — Board Governance — identifies that boards should review key strategic risks in corporate risk registers and set risk appetite.
- 16 April 2020 — Rapid Implementation of Australian Government Initiatives — outlines that risk rapid implementation may require a different risk appetite and treatments to those in more normal times.
- 24 June 2020 — Fraud Control Arrangements — identifies that fraud risks should be reviewed and assessed regularly. It also discusses the promotion of a fraud aware culture.
- 14 January 2021 — Administering Regulation — considers implementation of risk-based compliance programs in a regulatory environment.
- 28 May 2021 — Emergency Management — Insights from the Australian Government's COVID-19 Response — considers how to identify and manage implementation risk in a crisis or emergency.
- 25 January 2022 — Service Delivery through Other Entities — considers risk management in a service delivery context, particularly in relation to shared risks.
- 3 April 2023 — Procurement and Contract Management — considers risk management in procurement and contract management.
- 14 June 2023 — Cyber Security — considers risk as part of complying with the Protective Security Policy Framework and in managing cyber security.
- 16 October 2023 — Probity Management: Lessons from Audits of Financial Regulators — examines how entities can manage probity-related risks.

Other ANAO publications

- Strategic governance of risk: Lessons learnt from public sector audit
- Risk Management Framework 2022–24
- Risk Management Framework 2025–27

Department of Finance resources for risk management

- Commonwealth Risk Management Policy
- Risk Management Services (which includes Resource Management Guide 211 Implementing the Commonwealth Risk Management Policy, the Risk Management Toolkit and other resources relating to risk management)

Other resources

- The international risk management standard — principles and guidelines (ISO31000:2018)
- Auditing Standard ASA 315 *Identifying and Assessing the Risks of Material Misstatement*