

# **The Management of Risk by Public Sector Entities**

## **Across Entities**

© Commonwealth of Australia 2017

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-282-2 (Print)

ISBN 978-1-76033-283-9 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <https://www.pmc.gov.au/government/its-honour>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Senior Executive Director  
Corporate Management Branch  
Australian National Audit Office  
19 National Circuit  
BARTON ACT 2600

Or via email:

[communication@anao.gov.au](mailto:communication@anao.gov.au).





Canberra ACT  
15 August 2017

Dear Mr President  
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit across entities titled *The Management of Risk by Public Sector Entities*. The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website—<http://www.anao.gov.au>.

Yours sincerely

A handwritten signature in black ink, reading 'Grant Hehir', is positioned above the printed name.

Grant Hehir  
Auditor-General

The Honourable the President of the Senate  
The Honourable the Speaker of the House of Representatives  
Parliament House  
Canberra ACT

## AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:  
**Australian National Audit Office**  
**GPO Box 707**  
**Canberra ACT 2601**

**Phone: (02) 6203 7300**  
**Fax: (02) 6203 7777**  
**Email: [ag1@anao.gov.au](mailto:ag1@anao.gov.au)**

ANAO reports and information about the ANAO are available on our website:  
<http://www.anao.gov.au>

### **Audit team**

Russell Coleman  
Alex Doyle  
Deanne Allan  
Renée Hall  
Michelle Page

# Contents

---

Summary .....	7
Background .....	7
Conclusion .....	9
Supporting findings .....	10
Areas for improvement and key learnings .....	12
Summary of entity responses .....	13
<b>Audit findings.....</b>	<b>15</b>
<b>1. Background .....</b>	<b>16</b>
Introduction .....	16
Commonwealth Risk Management Policy.....	16
Surveys of risk management practices in the Australian Public Sector .....	19
Audit coverage.....	24
Entities selected for inclusion in the audit .....	24
Audit objective and scope .....	27
<b>2. Application of the Commonwealth Risk Management Policy .....</b>	<b>28</b>
Have entities implemented the Commonwealth Risk Management Policy? .....	29
Did entities update their risk policy and framework in a timely manner following the issue of the Commonwealth Risk Management Policy? .....	35
Are entities' risk management frameworks developed with relevant stakeholder consultation, including arrangements to consult in a timely and effective manner? .....	38
Are responsibilities and accountabilities for risk management clearly defined? .....	38
Are entities' risk appetite and risk tolerance defined? .....	39
Is risk considered as part of key business decisions and operations? .....	41
Have entities established arrangements to manage shared risks? .....	43
Do entities have relevant capability to underpin the management of risk? .....	44
Are entities' risk management frameworks reviewed to continuously improve the management of risks? .....	47
Was risk addressed in entity corporate plans? .....	51
Areas for improvement .....	53
Appendix 1   Responses from the selected entities .....	56
Appendix 2   The Commonwealth Risk Management Policy requirements .....	64
Appendix 3   ANAO assessment of the selected entities' application of the Commonwealth Risk Management Policy elements .....	66
Appendix 4   Health's Enterprise Risk Appetite statement .....	89



# Summary

---

## Background

1. The *Public Governance, Performance and Accountability Act 2013* (PGPA Act) places a duty on Accountable Authorities<sup>1</sup> of Commonwealth entities to establish and maintain appropriate systems of risk oversight and management for the entity.<sup>2</sup> To promote a coherent approach to discharging these duties and to assist Commonwealth entities to understand the requirements for managing risk, the Australian Government released the Commonwealth Risk Management Policy (Commonwealth Policy) on 1 July 2014 as an element of the Public Management Reform Agenda (PMRA).

2. One of the guiding principles of the PMRA reforms is that ‘engaging with risk is a necessary first step in improving performance’, and one of the lasting benefits that the reforms are seeking to deliver is ‘a more mature approach to risk across the Commonwealth’.<sup>3</sup> The effective management of risks assists Commonwealth entities and companies to:

- set and achieve strategic objectives;
- comply with legal and policy obligations;
- improve decision making; and
- allocate and utilise resources.

3. The Joint Committee of Public Accounts and Audit (JCPAA) highlighted, in its recent report on Commonwealth Risk Management, that risk management should be an integral part of the way the Australian public sector conducts business.<sup>4</sup>

## Commonwealth Risk Management Policy

4. The Commonwealth Policy defines risk as ‘the effect of uncertainty on objectives’ and risk management as the ‘coordinated activities to direct and control an organisation with regard to risk’.<sup>5</sup> The goal of the Commonwealth Policy is to embed risk management as part of the culture of Commonwealth entities where the shared understanding of risk leads to well informed decision making.<sup>6</sup>

5. The Commonwealth Policy advises that risk culture is the set of shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities. A positive risk culture: promotes an open and proactive approach to managing risk that considers both

---

1 An Accountable Authority for a Commonwealth entity is generally the person or group of persons that has responsibility for, and control over, the entity’s operations. Sub-section 12(2) of the PGPA Act sets out the person(s) or body that is the Accountably Authority of a Commonwealth entity.

2 *The Public Governance, Performance and Accountability Act 2013*, section 16.

3 Explanatory Memorandum to the *Public Governance, Performance and Accountability Bill 2013*, paragraphs 16 and 18.

4 JCPAA, *Report 461 Commonwealth Risk Management, Inquiry based on Auditor-General’s report 18 (2015-16)*, May 2017, paragraph 1.2.

5 Department of Finance, *Commonwealth Risk Management Policy*, Finance, 2014, paragraph 2.

6 *ibid.*, paragraph 7.

threat and opportunity; and is one where risk is appropriately identified, assessed, communicated and managed across all levels of the entity.<sup>7</sup>

6. Non-corporate Commonwealth entities, which include departments of state and most regulatory bodies, must comply with the Commonwealth Policy. Corporate Commonwealth entities are not required to comply with the policy, but are expected to review and align their risk management frameworks and systems with the policy as a matter of good practice.

7. The Commonwealth Policy mandates 22 specific requirements organised in nine policy elements. The policy elements are summarised in Box 1 and reproduced in Appendix 2.

Box 1: Policy Elements—Commonwealth Risk Management Policy
Element 1: Establishing a risk management policy – <i>four requirements</i>
Element 2: Establishing a risk management framework – <i>nine requirements</i>
Element 3: Defining responsibility for managing risk – <i>three requirements</i>
Element 4: Embedding systematic risk management into business processes
Element 5: Developing a positive risk culture
Element 6: Communicating and consulting about risk
Element 7: Understanding and managing shared risk
Element 8: Maintaining risk management capability
Element 9: Reviewing and continuously improving the management of risk

**Audit objective and criteria**

8. The objective of the audit was to assess how effectively selected public sector entities manage risk. To form a conclusion against the audit objective, the ANAO adopted the following high-level audit criteria:

- the selected entities’ risk management policies and frameworks meet the requirements of the Commonwealth resource management framework, including the Commonwealth Risk Management Policy;
- the selected entities’ business operations and key business processes are informed by considerations of risk; and
- the selected entities have established a supporting risk culture.

9. This performance audit is one of three audits in the ANAO’s work program that address key aspects of the implementation of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). These audits have been identified by the Joint Committee of Public Accounts and Audit (JCPAA) as priorities of the Parliament and will assist in keeping the Parliament, government and the community informed on implementation of the resource, risk and performance management frameworks introduced by the PGPA Act.

<sup>7</sup> *ibid.*, paragraphs 17–18.



10. Four non-corporate Commonwealth entities were selected for inclusion in the audit: the Department of Employment (Employment), the Department of Health (Health), the Australian Communications and Media Authority (ACMA), and the Australian Fisheries Management Authority (AFMA).

## Conclusion

11. The four entities involved in the audit have met or mostly met the majority of the 22 specific requirements of the Commonwealth Risk Management Policy, with further work required by three entities (Health, ACMA and AFMA) to fully realise the Policy's goal of embedding risk management as part of the entity's culture, where the shared understanding of risk leads to well-informed decision making.

- Employment has a mature and integrated approach to the identification and management of risk and has implemented a range of measures to build its risk capability, including an enterprise-wide risk management system. There is entity-level oversight of the operation of the risk management policy and framework through an internal governance committee which has reported regularly to the department's Executive Committee on the adequacy of the risk framework and associated processes.
- Health has an ongoing program to strengthen and fully operationalise its risk management framework and capability, following reviews in 2014 and 2016 which identified scope for improvement. Key risks are regularly considered by Health's Executive Committee in its consideration of specific departmental strategies and plans. There remains scope for a more structured approach to reporting on and reviewing enterprise-level risks and the status of risk controls and treatments.
- ACMA's key risks are reviewed quarterly by the senior executive as part of a regular cycle, and the Authority is in the process of reviewing its risk management policy. ACMA included a risk tolerance statement in its 2015 risk management guide but has not yet developed a risk appetite statement. ACMA's risk management guidance provides a high-level description of risk management, but limited practical guidance on how staff should manage risk.
- Sustainability risks were regularly considered by the AFMA Commission in its consideration of specific fisheries management strategies and plans. As with Health, there remains scope for a more structured approach to reporting on and reviewing enterprise-level risks, controls and treatments. Risk management guidance available on the Authority's intranet was minimal and not up to date, and AFMA does not have formal learning and development programs in risk management for staff. The Authority should address these impediments to the development of a positive risk management culture.

12. Each of the selected entities has continued to develop its risk management policies, framework and capability since the release of the Commonwealth Policy in July 2014. As a result of these efforts Employment has met, and Health and ACMA have mostly met, the requirement of policy element five and the overarching goal of the Commonwealth Policy—relating to the development of a positive and embedded risk culture. AFMA has partly met the requirement of policy element five and the overarching policy goal.

13. A number of areas for improvement have been identified for the selected entities, and more general matters which may also warrant attention by other Commonwealth entities. The two categories of learnings address: for the selected entities, measures which would improve compliance with the policy requirements; and, for all public sector entities, key learnings focusing on strengthening risk management capability, culture and performance.

## Supporting findings

### Implementation

14. The four selected entities have met or mostly met the majority of the 22 mandated requirements of the Commonwealth Risk Management Policy (Commonwealth Policy)<sup>8</sup>:

- the Department of Employment (Employment) met 19 and mostly met two of the requirements (total 21/22 or 95 per cent);
- the Department of Health (Health) met 10 and mostly met 10 of the requirements (total 20/22 or 91 per cent);
- the Australian Communications and Media Authority (ACMA) met six and mostly met 10 of the requirements (total 16/22 or 73 per cent); and
- the Australian Fisheries Management Authority (AFMA) met 13 and mostly met two of the requirements (total 15/22 or 68 per cent).

### Risk policy and framework

15. Each of the selected entities released an updated risk policy and framework within 12 months of the release of the Commonwealth Risk Management Policy. The selected entities have also continued to update elements of their policy and framework (Employment and AFMA) or have plans to do so (Health and ACMA).

### Stakeholder consultation

16. The selected entities' risk management frameworks were developed with extensive internal consultation, including with audit committees. There remains scope for entities to include, in their risk framework documentation, their arrangements for communicating, consulting and reporting on risk to both their internal and external stakeholders.

### Responsibilities

17. For three entities, responsibilities for managing and reporting on risk are clearly identified (Employment, Health and AFMA). ACMA has documented some, but not all, responsibilities.

---

8 The Commonwealth Policy mandates the implementation of 22 specific requirements organised in nine elements.

## Defining risk appetite and tolerance

18. Three of the selected entities developed new or revised risk appetite and tolerance statements following the release of the Commonwealth Policy (Employment, Health and AFMA). One entity included a risk tolerance statement in its 2015 risk management guide, but has not developed a risk appetite statement (ACMA).

## Considering risk in business decisions and operations

19. The risk framework and key risks were regularly considered at senior levels within the selected entities. There is scope for a more structured approach to reporting on and reviewing enterprise-level risks and the status of risk controls and treatments (Health and AFMA). At present there is limited management reporting to the Executive Committee (Health) or Commission (AFMA) on enterprise-level risks, and no reporting on operational risks to the Audit and Risk Committee (Health and AFMA).

20. The ANAO's review of a selection of business activities in each entity indicates that risk management also informs normal business operations. Risk was considered when key business decisions were made or advice was provided to senior management or government in the areas selected for review.

## Managing shared risk

21. The identification and management of shared risks is one of the least mature elements of entities' implementation of the Commonwealth Policy. Shared risks are not routinely identified and managed as such in the context of entities' risk management policies and frameworks (Health, ACMA and AFMA).

## Risk management capability

22. The selected entities have implemented a range of measures to build their risk management capability. Key measures include:

- regular internal reporting on the entity's risk profile and risk framework (Employment and ACMA);
- risk management guidance, templates and dedicated risk hot lines or email addresses (Employment, Health and ACMA);
- staff resources dedicated to risk management (Employment, Health);
- custom-built risk management systems (Employment); and
- learning and development programs which address risk management, including eLearning modules (Employment, Health and ACMA).

## Review activity

23. The selected entities' risk management policies include a commitment to regularly review the risk framework, and each of the entities has continued to review its risk management policies and framework since the Commonwealth Policy was released in July 2014.

## Corporate plans

24. The selected entities were at different levels of maturity in their implementation of the corporate plan requirement relating to risk, with further work required in all entities to fully embed the requirement.

## Areas for improvement and key learnings

25. Based on the audit findings, the Australian National Audit Office has identified areas for improvement on a range of matters which warrant further attention by the selected entities, and key learnings that could be applied by other public sector entities. The two categories of learnings presented in Box 2 and Box 3 address the Commonwealth Policy's goal of embedding risk management as part of an entity's culture, where the shared understanding of risk leads to well informed decision making.

### Box 2: Areas for improvement for the selected entities

- Defining the entity's risk appetite in the risk management policy (ACMA).
- Enhancing risk management capability (Health, ACMA and AFMA).
- Improving the identification and management of shared risks (all entities).
- Developing arrangements for communicating, consulting and reporting on risk with internal and external stakeholders (all entities).
- Improving arrangements to regularly review risks, risk management frameworks and the application of risk management practices (Health, ACMA and AFMA).
- Seeking formal assurance from managers in preparing entity responses to the Comcover survey of risk maturity (all entities).
- Fully embedding the corporate plan requirement relating to risk (all entities).
- Assigning responsibility for risk management to individuals or positions, rather than work areas (Health, ACMA and AFMA).

**Box 3: Key learnings that could be applied by other public sector entities**

- Regular management reporting on risk—including enterprise-level risks and the status of risk controls and treatments—helps provide assurance on risk management.
- Regular and structured review of risk—including enterprise-level risks and the status of risk controls and treatments by governance committees, the executive board and the audit committee—contributes to embedding systematic risk management into business processes.
- Updating guidance and templates to reflect the entity's risk appetite and tolerance supports the development of a positive risk culture.
- Providing practical guidance on how staff should manage risk contributes to building internal risk management capability.
- Establishing strategies to improve participation in risk-related learning and development programs, including the completion of eLearning modules, helps maintain risk management capability.
- In considering shared risks, focus on shared outcome risks rather than low level transactional risks.
- Recording and analysing risk incidents and lessons learned can provide valuable insights to management and the audit committee on risk management performance and the effectiveness of the risk management framework.
- Consider mechanisms to measure risk management performance.

**Summary of entity responses**

26. The Department of Employment, the Department of Health, the Australian Communications and Media Authority, the Australian Fisheries Management Authority, and the Department of Finance were provided with a copy of the proposed audit report, and the Australian Public Service Commission was provided with an extract of the proposed report for comment. A summary of the responses received from entities is provided below, with the full responses provided at Appendix 1.

**Department of Employment**

The Department of Employment (the Department) welcomes the overall findings of the Australian National Audit Office's (the ANAO) Performance Audit of the Management of Risk by Public Sector Entities (the audit).

The Department recognises risk management is a cornerstone of good corporate governance and organisational success. Managing risk well enables us to achieve our outcomes and promotes the efficient, effective and ethical use of Australian Government resources. The audit concludes the Department has a mature and integrated approach to the identification and management of risk and has implemented a range of measures to build its risk capability. The Department has consciously invested in its risk management framework and I am pleased the ANAO has identified the positive returns from this investment.

The process of mature risk management is ongoing and we will take action in relation to areas for improvement identified in the audit that relate to the Department.

## **Department of Health**

I am pleased that the ANAO found that the Department of Health (Health) has met a substantial number of the requirements of the Commonwealth Risk Management Policy. The report demonstrates the progress Health has made to improve its risk management approach and shift to a more risk aware culture. Shifting an organisation's risk culture requires significant commitment from all levels within the organisation and takes time.

In April 2017, Health's Accountability Authority endorsed and released a revised Risk Management Policy. This Policy articulates our approach to building a culture of effective risk engagement, where each of us has the skills and confidence to identify and manage risks appropriately.

The report has highlighted several areas for improvement in order to strengthen the systems and culture that are required to embed a risk aware culture. Health agrees with these findings and will implement actions to facilitate improvement in these areas.

## **Australian Communications and Media Authority**

The findings are timely as the ACMA Risk Management Framework is currently under review and we will keep the ANAO's findings front of mind while making refinements to this framework.

As part of our review, we have already taken steps to address some of the areas for improvement identified by the ANAO. Our Executive Group is releasing a revised Risk Appetite Statement and we are working to ensure our agency has the capability to engage effectively with risk.

The Executive Group has started the discussion to establish an enduring policy position on the identification and management of shared risk.

We have appointed a Chief Risk Officer to drive improvements to the Risk Management Framework and provide additional support to staff.

There is a strong culture of risk management within the ACMA. The insights provided by the ANAO will help us to refine our Risk Management Framework in a way that best supports and builds on that culture.

## **Australian Fisheries Management Authority**

The Australian Fisheries Management Authority (AFMA) acknowledges the supported findings and areas of improvement outlined in this report. AFMA has recently reviewed our Risk Management Policy and Risk Management Guidelines and the report will greatly assist in their full implementation.

## **Department of Finance**

The Department of Finance supports the findings of this report.

# Audit findings

# 1. Background

---

## Introduction

1.1 The *Public Governance, Performance and Accountability Act 2013* (PGPA Act) places a duty on Accountable Authorities<sup>9</sup> of Commonwealth entities to establish and maintain appropriate systems of risk oversight and management for the entity.<sup>10</sup> To promote a coherent approach to discharging these duties and to assist Commonwealth entities to understand the requirements for managing risk, the Australian Government released the Commonwealth Risk Management Policy (Commonwealth Policy) on 1 July 2014 as an element of the Public Management Reform Agenda (PMRA).

1.2 One of the guiding principles of the PMRA reforms is that ‘engaging with risk is a necessary first step in improving performance’, and one of the lasting benefits that the reforms are seeking to deliver is ‘a more mature approach to risk across the Commonwealth’.<sup>11</sup> The effective management of risks assists Commonwealth entities and companies to:

- set and achieve strategic objectives;
- comply with legal and policy obligations;
- improve decision making; and
- allocate and utilise resources.

1.3 The Joint Committee of Public Accounts and Audit (JCPAA) highlighted, in its recent report on *Commonwealth Risk Management*, that risk management should be an integral part of the way the Australian public sector conducts business.<sup>12</sup>

## Commonwealth Risk Management Policy

1.4 The Commonwealth Policy defines risk as ‘the effect of uncertainty on objectives’ and risk management as the ‘coordinated activities to direct and control an organisation with regard to risk’.<sup>13</sup> The Commonwealth Policy has 22 requirements organised in nine policy elements. The nine elements of the Commonwealth Policy are presented in Figure 1.1.

---

9 An Accountable Authority for a Commonwealth entity is generally the person or group of persons that has responsibility for, and control over, the entity’s operations. Sub-section 12(2) of the PGPA Act sets out the person(s) or body that is the Accountably Authority of a Commonwealth entity.

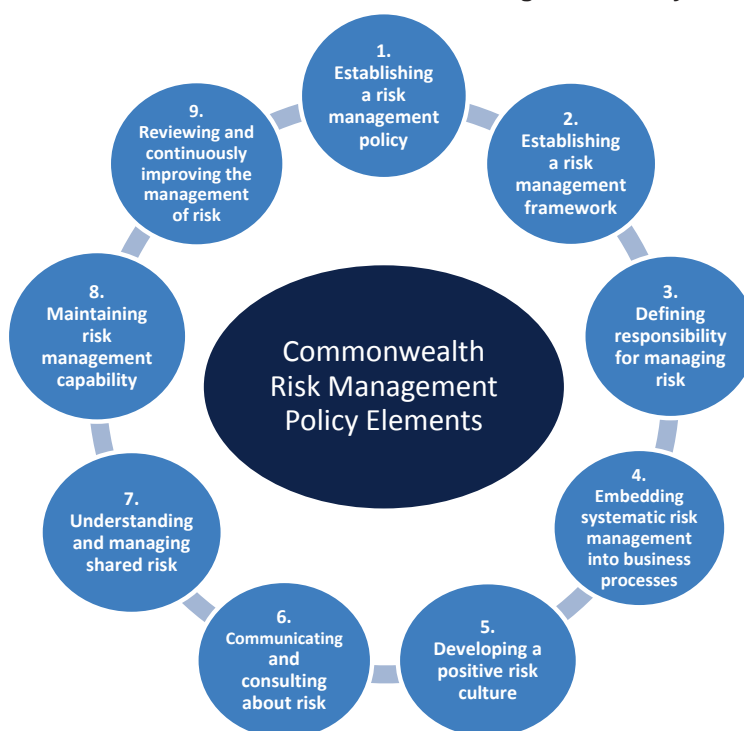
10 *The Public Governance, Performance and Accountability Act 2013*, section 16.

11 Explanatory Memorandum to the *Public Governance, Performance and Accountability Bill 2013*, paragraphs 16 and 18.

12 JCPAA, *Report 461 Commonwealth Risk Management, Inquiry based on Auditor-General’s report 18 (2015–16)*, May 2017, paragraph 1.2.

13 Department of Finance, *Commonwealth Risk Management Policy*, Finance, 2014, paragraph 2.



**Figure 1.1: Elements of the Commonwealth Risk Management Policy**

Note: Elements 1–3 of the Commonwealth Policy are comprised of multiple requirements. The mandatory requirements of the Commonwealth Policy are outlined at Appendix 2.

Source: ANAO presentation of the Commonwealth Risk Management Policy.

1.5 The goal of the Commonwealth Policy is to embed risk management as part of the culture of Commonwealth entities where the shared understanding of risk leads to well informed decision making.<sup>14</sup> Element five of the policy also provides that an entity's risk management framework must support the development of a positive risk culture.

1.6 The policy advises that risk culture is the set of shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities. A positive risk culture: promotes an open and proactive approach to managing risk that considers both threat and opportunity; and is one where risk is appropriately identified, assessed, communicated and managed across all levels of the entity.<sup>15</sup>

1.7 Professor Peter Shergold AC has observed that the PGPA Act 'represents a significant and positive step towards developing better risk practice and culture. The risk management policy established under the PGPA Act is designed to assist Accountable Authorities ... to engage positively with risk, in order to embed risk practice into business processes'.<sup>16</sup>

14 *ibid.*, paragraph 7.

15 *ibid.*, paragraphs 17–18.

16 Australian Public Service Commission, *Learning from Failure*, August 2015, p. 37.

1.8 Non-corporate Commonwealth entities, which include all departments of state, must comply with the Commonwealth Policy. Corporate Commonwealth entities are not required to comply with the policy, but are expected to review and align their risk management frameworks and systems with the policy as a matter of good practice.

1.9 A review of the Commonwealth Policy was originally scheduled to occur in 2015—a year after its release. This was deferred following recognition that entities needed time to align their frameworks to the Commonwealth Policy. The review is now scheduled to align with the review of the PGPA Act.<sup>17</sup>

### **Related requirements**

1.10 The PGPA Act also introduced the requirement that entities produce annual corporate plans and report on entity performance in annual performance statements. The PGPA Rule 2014, made pursuant to the Act, provides that an entity's corporate plan must provide a summary of the risk oversight and management systems of the entity for each reporting period covered by the plan (section 16E).

1.11 The PGPA Rule 2014 also provides that the functions of an entity's audit committee must include reviewing the appropriateness of the accountable authority's system of risk oversight and control.<sup>18</sup>

### **Comparison with the Australian/New Zealand Risk Standard and risk management frameworks in other jurisdictions**

1.12 The Commonwealth Risk Management Policy references relevant risk standards<sup>19</sup> and is consistent with the standard jointly published by Standards Australia and Standards New Zealand, *Risk management—principles and guidelines*.<sup>20</sup>

1.13 Other jurisdictions in Australia and internationally also publish public sector risk management policies and/or guidance to assist entities. This material is framed by each jurisdiction's legislative framework and policy responsibilities. The Commonwealth Policy and associated guidance is broadly consistent with the risk management material published by other jurisdictions that was reviewed by the ANAO.<sup>21</sup> For example, defining risk appetite and/or tolerance, the importance of communication, consultation and shared risks are common elements of policy and guidance in a number of jurisdictions, such as NSW and Canada.

---

17 A review of the PGPA Act is required under section 112 of that Act. The effect of section 112 is to require the Finance Minister, in consultation with the Joint Committee of Public Accounts and Audit, to conduct a review of the PGPA Act and the PGPA Rules as soon as practicable after 1 July 2017.

18 The ANAO survey of the PGPA Rule is discussed in ANAO Report No.33 2016–17 *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2016*.

19 While not mandatory, an entity's risk management framework and systems should be aligned with and reflect existing standards and guidance such as *AS/NZS ISO 31000:2009—Risk management—principles and guidelines*.

20 *AS/NZS ISO 31000:2009* was published in 2009 and is identical with *ISO 31000:2009 Risk Management—Principles and Guidelines* published by the International Organization for Standardization.

21 The ANAO reviewed the risk management policy and guidance published by New South Wales, Victoria, Western Australia, Queensland, South Australia, the United Kingdom, Canada and New Zealand.

1.14 While risk management is not new to the Commonwealth public sector<sup>22</sup>, the implementation of a mandated risk management policy is a new development and not one that has been adopted and tested in comparable administrative systems. The United Kingdom for instance released a risk management framework in January 2017, which provides high level guidance rather than a mandated policy.<sup>23</sup> Similarly, the Canadian and New Zealand Governments each have a broad, principled framework for the management of risk rather than a policy with mandatory requirements.

## Surveys of risk management practices in the Australian Public Sector

1.15 Australian Government entities are required to submit a self-assessment of their risk management capability for the purposes of Comcover's annual *Risk Management Benchmarking Survey*. In addition the Australian Public Service Commission (APSC) undertakes the annual Australian Public Service (APS) employee census and the annual agency survey, which have included questions on risk management.

### Risk Management Benchmarking Survey

1.16 The Department of Finance (Comcover)<sup>24</sup> has conducted an annual benchmarking program since 2001. The Risk Management Benchmarking Survey is a tool to assist entities self-assess their risk management capability against each of the nine elements outlined in the Commonwealth Policy (see Figure 1.1).

1.17 The 2016 Risk Management Benchmarking Survey (the survey) was open for completion from 18 January to 4 March 2016. A total of 143 Australian Government (non-Corporate) entities participated in the survey in 2016 by submitting a self-assessment rating of their risk management capability using a six level risk maturity model, as illustrated in Figure 1.2.

- 
- 22 In the Foreword to the 2014 Commonwealth Policy, the Minister for Finance observed that the nine policy elements would assist accountable authorities to build on their existing risk management framework. Whole-of-government guidance on risk management has been available to the Australian Public Service for some decades—see, for example, guidance published by the Australian Public Service Management Advisory Board (MAB) and its supporting Management Improvement Advisory Committee (MIAC), MAB/MIAC Report No.22, *Guidelines for Managing Risk in the Australian Public Service*, AGPS, October 1996.
- 23 United Kingdom Cabinet Office, *Management of Risk in Government Framework—a framework for boards and examples of what has worked in practice*, January 2017, available at <https://www.gov.uk/government/publications/management-of-risk-in-government-framework> [accessed 3 April 2017]
- 24 Comcover is the Australian Government's self-managed insurance fund in the Department of Finance, that provides insurance and risk management services to Commonwealth General Government Sector entities. A key function of Comcover is to assist entities to build their capability to manage risk across the Australian Government. Comcover has stated that it aims to enable entities to obtain the knowledge, skills and expertise that will assist them to successfully implement and integrate risk management within their organisation.

Figure 1.2: Six level risk maturity model rating



Note: While a risk maturity rating level indicates where there is still scope to improve risk management capabilities, it is not a ‘compliance rating’.

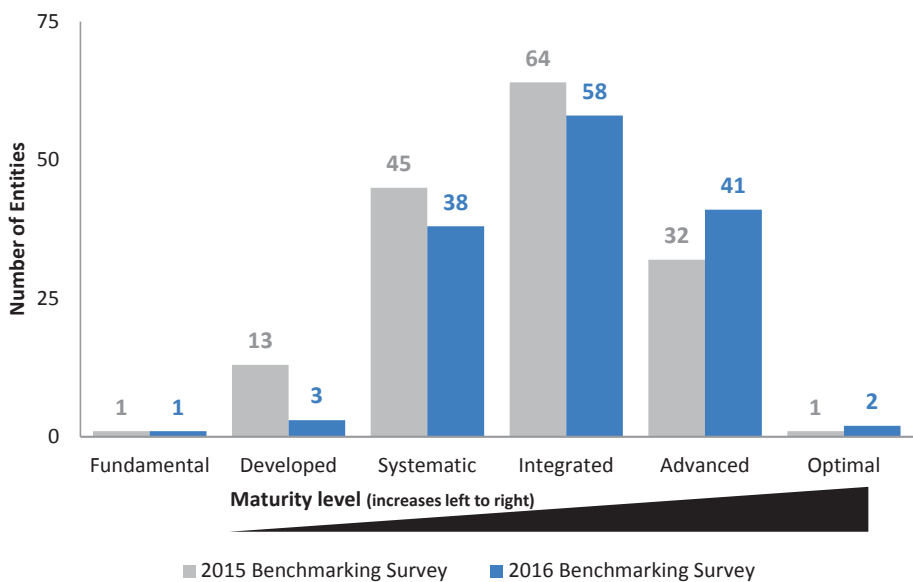
Source: Risk Management Benchmarking Program 2016: Comcover's Key Findings Report.

1.18 Entities are encouraged to adopt risk maturity ratings that are fit for purpose for their organisation. Not all entities are expected to achieve an ‘optimal’ rating, and entity maturity levels are not a ‘compliance’ rating.

1.19 In the 2016 survey, 67 per cent of entities self-reported a maturity level of *Systematic* or *Integrated*, and 30 per cent of entities reported achievements of *Advanced* or *Optimal* maturity. Comcover observed in its key findings report that a general shift towards higher overall risk maturity levels across the entities in 2016 from 2015 (Figure 1.3) indicates that many entities have made progress in building their risk management capability over the last year.

1.20 The distribution of the maturity levels achieved by participating entities in the 2016 benchmarking survey is illustrated in Figure 1.3.

Figure 1.3: Distribution of maturity levels achieved by participating entities—Comcover risk benchmarking survey



Source: ANAO reproduction of data presented in the Risk Management Benchmarking Program 2016: Comcover's Key Findings Report.

1.21 Comcover has observed that the findings of the 2016 survey indicate that 88 per cent of entities have a risk management policy that has been endorsed by their accountable authority and is aligned with their corporate plan and objectives. According to Comcover, the survey indicates that 'while there are pockets of well embedded risk management practice, there is still room to improve how well risk management is embedded into strategic planning, governance arrangements and program delivery.'

1.22 Comcover noted that the 2016 survey results indicate that the highest performing elements of the Commonwealth Policy across the population of entities were:

- Element 1 – Establishing a risk management policy;
- Element 3 – Defining responsibility for managing risk; and
- Element 4 – Embedding systematic risk management into business processes.

1.23 Comcover further noted that the 2016 survey results indicated that the Commonwealth Policy elements that were the lowest scoring elements across the population of entities were:

- Element 5 – Developing a positive risk culture;
- Element 7 – Understanding and managing shared risk; and
- Element 8 – Maintaining risk management capability.

1.24 Key insights and the maturity distribution across the surveyed population of entities for each element of the Commonwealth Risk Management Policy are illustrated in Figure 1.4.

**Figure 1.4: Key insights and maturity distribution across the surveyed population for each element of the Commonwealth Risk Management Policy**



Source: Risk Management Benchmarking Program 2016: Comcover's Key Findings Report.

## Australian Public Service Commission data

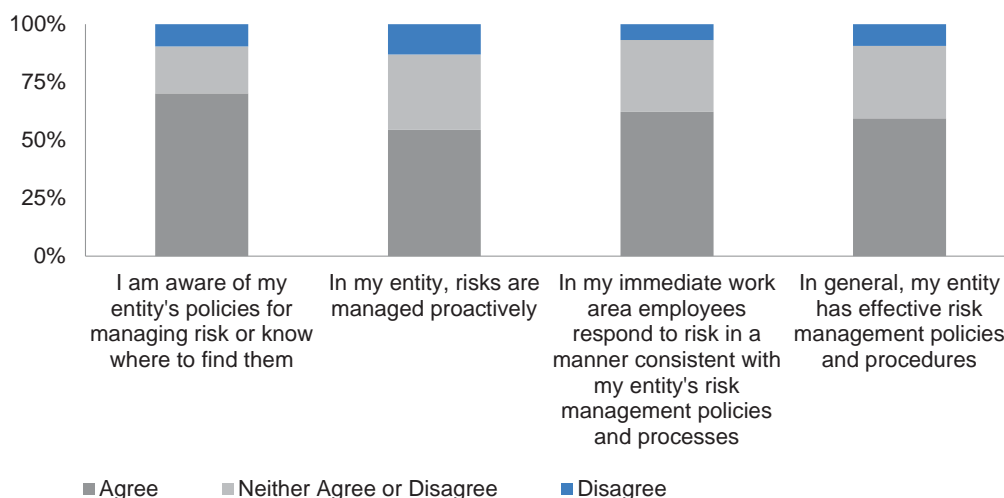
1.25 The Australian Public Service Commission (APSC) surveys APS agencies and employees annually on a range of workforce management issues. Both surveys have included a number of questions relating to risk management.

1.26 The self-assessments by APS agencies indicate that:

- 48 per cent of surveyed entities had plans to improve risk management during 2016;
- 39 per cent of surveyed entities considered that no action was necessary to improve risk management in their entity;
- 19 per cent of surveyed entities reported that no barriers existed to improving risk management capability in 2016; and
- the main challenges to improving risk management capability were:
  - resource availability and consistency of risk management practices (17 per cent);
  - limited resource availability (15 per cent); and
  - enhancing risk management frameworks and practices (11 per cent); and
- surveyed employees were less positive in 2016 compared with 2015 about entities' risk management practices.

1.27 A summary of the results of the APS employee census is presented in Figure 1.5.

**Figure 1.5: Summary results for all employees surveyed by the APSC in 2016**



Source: ANAO analysis of 2016 APS employee census responses.

## Audit coverage

1.28 This performance audit is one of three audits in the ANAO's work program that address key aspects of the implementation of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). The other two audits are:

- Report No.54 2016–17 *Corporate Planning in the Australian Public Sector*. This performance audit is the second in a series of audits that assessed progress in implementing the corporate planning requirement under the PGPA Act. The first in the series was Report No.6 2016–17 *Corporate Planning in the Australian Public Sector*; and
- Report No.58 2016–17 *Implementation of the Annual Performance Statements Requirements 2015–16*. This audit assessed the performance statements included in the 2015–16 Annual Reports of the Department of Agriculture and Water Resources and the Australian Federal Police.

1.29 These audits have been identified by the Joint Committee of Public Accounts and Audit as priorities of the Parliament and will assist in keeping the Parliament, government and the community informed on implementation of the resource, risk and performance management frameworks introduced by the PGPA Act.

## Entities selected for inclusion in the audit

1.30 Four non-corporate Commonwealth entities were selected for inclusion in the audit:

- two departments of state—the Department of Employment (Employment) and the Department of Health (Health); and
- two regulatory bodies— the Australian Communications and Media Authority (ACMA) and the Australian Fisheries Management Authority (AFMA).

1.31 Table 1.1 contains additional information about the selected entities.



**Table 1.1: Information about the selected entities**

Department of Employment
<p>The Department of Employment (Employment) is a large entity, with around 1985 staff at 30 June 2016. Employment had a total budget of approximately \$2.4 billion in 2015–16.</p> <p>Employment's role is to provide national policies and programs that help Australians find and keep employment, work in safe, fair and productive workplaces, and improve the employment-related performance of enterprises in Australia.</p> <p>The department has identified the following enterprise level risks:</p> <ul style="list-style-type: none"> <li>• Loss of confidence in the department as a result of the failure to manage portfolio issues in a manner consistent with government policy and public sector management standards [Reputational risk].</li> <li>• A change to resources or capabilities renders the Department unable to deliver on budget, on time and to expectations [Implementation and service delivery risk].</li> <li>• Insufficient stakeholder engagement undermines policy development and outcomes [Customer service risk].</li> <li>• A major system failure results in the department being unable to deliver core business priorities [Information technology risk].</li> <li>• A need to meet urgent priorities with constrained resources undermines strategic thinking, collaboration and program assurance, leading to diminished policy innovation and delivery [Strategic thinking risk].</li> <li>• A fraud event is not prevented or detected [Fraud risk].</li> </ul>
Department of Health
<p>The Department of Health (Health) is a large entity, with around 5037 staff at 30 June 2016. Health had a total budget of approximately \$54.3 billion in 2015–16.</p> <p>Health is responsible for achieving the Australian Government's health priorities through evidence-based policy, program administration, research, regulatory activities and partnerships with other government entities, consumers and stakeholders.</p> <p>The department has identified the following enterprise level risks:</p> <ul style="list-style-type: none"> <li>• The department's regulatory policies and practices are not able to adequately protect the health and safety of the community and/or, reduce excessive regulatory burden on business, healthcare professionals and consumers [Regulatory risk].</li> <li>• Inadequate assessment and management of the health and wellbeing of our people and in particular departmental inspectors, investigators and laboratory staff, resulting in diminished productivity, disengagement or injury [People risk].</li> <li>• Failure to recognise and respond to inappropriate influence or corruption of a public official leading to loss of confidence in the department and diversion of resources from intended purposes [Fraud risk].</li> <li>• The department's health system strategy and implementation (short, medium and long term) is insufficient to mitigate the growth in outlays [Policy risk].</li> <li>• Inadequate capability and tools to collect and utilise data sets and health system information to optimise health, ageing and sport policy outcomes [Policy risk].</li> <li>• Co-ordination and integration of policy and programs across the department and external partners are insufficient, leading to poor outcomes for the community and/or an adverse budgetary effect [Delivery risk].</li> <li>• Failure to learn through measuring and evaluating policies, programs and service outcomes [Delivery risk].</li> <li>• Failure to ensure resources are allocated to the highest priorities of the Minister and the Department in a responsive and adaptive way [Governance risk].</li> </ul>

### Department of Health (continued)

- Failure to promptly recognise the impact of poor data management, IT capacity and lack of skilled staff on the delivery of health and ageing services [Delivery risk].
- Failure to recognise or respond promptly, proactively and effectively to an interruption of delivery of Commonwealth funded health and ageing services to the community [Delivery risk].
- Governance arrangements don't support the provision of timely, accurate and robust advice [Governance risk].
- Poor IT stability and security leads to ineffective and inefficient Health administration or unauthorised access to personal data [Information risk].

### Australian Communications and Media Authority

The Australian Communications and Media Authority (ACMA) is a small entity, with around 446 staff at 30 June 2016. ACMA had a total budget of approximately \$93.4 million in 2015–16.

ACMA sits within the Department of Communications and the Arts portfolio. ACMA's mandate is to deliver a communications and media environment that balances the needs of industry and the Australian community through regulation, education and advice. The Authority's purpose is to ensure communications and media work is in Australia's public interest and is achieved with a judicious blend of communication, facilitation and regulation.

The department has identified the following enterprise level risks:

- Fails to identify and develop relevant responses to a rapidly changing and evolving media and communications environment [Environmental responsiveness risk].
- Regulatory strategy, priorities and approach are not consistent with the expectations or objectives of the government's media and communications regulation and strategy [Regulatory strategy risk].
- Fails to provide well-considered and timely advice to government to support sound media and communications regulation outcomes for all Australians [Relationship with government risk].
- ACMA is perceived as ineffective or irrelevant by key regulated entities in industry, hampering its ability to achieve regulatory outcomes [Relationship with industry risk].
- Public lose confidence in the ACMA's ability to perform its statutory role in the communications and media sectors, reducing its effectiveness [Relationship with consumers/citizens risk].
- Failure of the ACMA's organisational capability (research, engagement, response, corporate support) affects its ability to achieve effective regulatory outcomes; or leads to a perception that the ACMA does not make a relevant contribution to the Australian media and communications environment, reducing its effectiveness [Organisational capability risk].
- Regulatory strategy and/or delivery (use of components of regulatory toolkit) is either inappropriate or ineffective [Ineffective regulatory delivery risk].

### Australian Fisheries Management Authority

The Australian Fisheries Management Authority (AFMA) is a small entity, with around 181 staff at 30 June 2016. AFMA had a total budget of approximately \$40 million in 2015–16.

AFMA sits within the Department of Agriculture portfolio, and was established in 1992 to manage Australia's Commonwealth fisheries and apply the provisions of the *Fisheries Administration Act 1991* and the *Fisheries Management Act 1991*. AFMA has offices in three locations—Canberra, Darwin and Thursday Island.

AFMA's 2016 Corporate Plan describes the composition of the risk management framework but does not identify enterprise level risks.

Source: ANAO analysis of data in entities' 2016–17 Corporate Plans.

## Audit objective and scope

1.32 The objective of the audit was to assess how effectively selected public sector entities manage risk. To form a conclusion against the audit objective, the ANAO adopted the following high-level audit criteria:

- the selected entities' risk management policies and frameworks meet the requirements of the Commonwealth resource management framework, including the Commonwealth Risk Management Policy;
- the selected entities' business operations and key business processes are informed by considerations of risk; and
- the selected entities have established a supporting risk culture.

1.33 In undertaking the audit, the ANAO:

- sought representations from entity management on entities' performance in relation to the audit objective;
- reviewed relevant documents, including the risk management policies and frameworks of the four entities;
- interviewed staff and reviewed relevant risk management records in a sample of business areas; and
- interviewed the chairs of entity audit committees.

1.34 In addition, the ANAO has drawn on:

- information obtained by the Australian Public Service Commission (APSC) through its data collections; and
- interviews with Department of Finance staff and records held by Finance in the context of its responsibilities as the policy owner of the resource management framework and Comcover's risk management responsibilities.

1.35 The ANAO applied part of its methodology developed for the recent series of audits of *Corporate Planning in the Australian Public Sector*.<sup>25</sup> The relevant part of the methodology was used to assess the maturity of the risk oversight and management section of entities' corporate plans.<sup>26</sup>

1.36 The audit was conducted in accordance with the ANAO Auditing Standards at a cost to the ANAO of approximately \$526 000.

1.37 The team members for this audit were Russell Coleman, Alex Doyle, Deanne Allan, Renée Hall and Michelle Page.

---

25 See paragraph 1.26 above.

26 See paragraphs 2.63 to 2.68.

## 2. Application of the Commonwealth Risk Management Policy

---

### Areas examined

The ANAO assessed implementation of the July 2014 Commonwealth Risk Management Policy (Commonwealth Policy) by the Department of Employment (Employment), the Department of Health (Health), the Australian Fisheries Management Authority (AFMA) and the Australian Communications and Media Authority (ACMA). The ANAO also assessed if the selected entities have met the goal of the Commonwealth Policy, which is to embed risk management as part of the culture of Commonwealth entities where the shared understanding of risk leads to well informed decision making.

### Conclusion

Each of the selected entities has continued to develop its risk management policies, framework and capability since the release of the Commonwealth Policy in July 2014. As a result of these efforts Employment has met, and Health and ACMA have mostly met, the requirement of policy element five and the overarching goal of the Commonwealth Policy—relating to the development of a positive and embedded risk culture. AFMA has partly met the requirement of policy element five and the overarching Policy goal.

### Areas for improvement

The ANAO has not made any recommendations in this audit, but has highlighted a range of matters which warrant further attention by the selected entities. The matters highlighted in this audit may also warrant attention by other Commonwealth entities.

Specific matters which warrant further attention by the selected entities relate to:

- defining the entity's risk appetite in the risk management policy (ACMA);
- enhancing risk management capability (Health, ACMA and AFMA);
- improving the identification and management of shared risks (all entities);
- developing arrangements for communicating, consulting and reporting on risk with internal and external stakeholders (all entities);
- improving arrangements to regularly review risks, risk management frameworks and the application of risk management practices (Health, ACMA and AFMA);
- seeking formal assurance from managers in preparing entity responses to the Comcover survey of risk maturity (all entities);
- fully embedding the corporate plan requirement relating to risk (all entities); and
- assigning responsibility for risk management to individuals or positions, rather than work areas (Health, ACMA and AFMA).

## Have entities implemented the Commonwealth Risk Management Policy?

The four selected entities have implemented the majority of the 22 mandated requirements of the Commonwealth Policy:

- the Department of Employment (Employment) met 19 and mostly met two of the requirements (total 21/22 or 95 per cent);
- the Department of Health (Health) met 10 and mostly met 10 of the requirements (total 20/22 or 91 per cent);
- the Australian Communications and Media Authority (ACMA) met six and mostly met 10 of the requirements (total 16/22 or 73 per cent); and
- the Australian Fisheries Management Authority (AFMA) met 13 and mostly met two of the requirements (total 15/22 or 68 per cent).

2.1 The Minister for Finance issued the *Commonwealth Risk Management Policy* (Commonwealth Policy) on 1 July 2014. Non-corporate Commonwealth entities must implement the Commonwealth Policy, which has 22 specific requirements organised in nine policy elements.

2.2 The ANAO's review of the selected entities' implementation of the Commonwealth Policy indicated that entities have met or mostly met the following percentage of requirements: Employment, 95 per cent; Health, 91 per cent; ACMA, 73 per cent; AFMA, 68 per cent. Table 2.1 summarises the number of requirements met or mostly met by the selected entities.

**Table 2.1: Number of mandated requirements met or mostly met by selected entities**

Entity	Met	Mostly met	Total	Percentage (n=22)
Employment	19	2	21	95
Health	10	10	20	91
ACMA	6	10	16	73
AFMA	13	2	15	68

Source: ANAO analysis.

2.3 Table 2.2 presents the ANAO's summary assessment of the selected entities' implementation of the nine policy elements of the Commonwealth Risk Management Policy.

**Table 2.2: ANAO’s summary assessment of selected entities’ implementation of the Commonwealth Risk Management Policy**

Elements of the Commonwealth Risk Management Policy		ANAO assessment			
<b>Element 1: Establishing a risk management policy—four requirements</b>					
Department of Employment					
Department of Health					
Australian Communications and Media Authority (ACMA)					
Australian Fisheries Management Authority (AFMA)					
<b>Element 2: Establishing a risk management framework—nine requirements</b>					
Department of Employment					
Department of Health					
Australian Communications and Media Authority (ACMA)					
Australian Fisheries Management Authority (AFMA)					
<b>Element 3: Defining responsibility for managing risk—three requirements</b>					
Department of Employment					
Department of Health					
Australian Communications and Media Authority (ACMA)					
Australian Fisheries Management Authority (AFMA)					
<b>Element 4: Embedding systematic risk management into business processes</b>					
Department of Employment					
Department of Health					
Australian Communications and Media Authority (ACMA)					
Australian Fisheries Management Authority (AFMA)					
<b>KEY:</b> <div> <div>Not met—no requirements met </div> <div>Partly met—some requirements met </div> <div>Mostly met—most requirements met </div> <div>Met—all requirements met </div> </div>					

Elements in the Commonwealth Risk Management Policy		ANAO assessment			
Element 5: Developing a positive risk culture					
Department of Employment					
Department of Health					
Australian Communications and Media Authority (ACMA)					
Australian Fisheries Management Authority (AFMA)					
Element 6: Communicating and consulting about risk					
Department of Employment					
Department of Health					
Australian Communications and Media Authority (ACMA)					
Australian Fisheries Management Authority (AFMA)					
Element 7: Understanding and managing shared risk					
Department of Employment					
Department of Health					
Australian Communications and Media Authority (ACMA)					
Australian Fisheries Management Authority (AFMA)					
Element 8: Maintaining risk management capability					
Department of Employment					
Department of Health					
Australian Communications and Media Authority (ACMA)					
Australian Fisheries Management Authority (AFMA)					
Element 9: Reviewing and continuously improving the management of risk					
Department of Employment					
Department of Health					
Australian Communications and Media Authority (ACMA)					
Australian Fisheries Management Authority (AFMA)					
KEY:		<div><div>Not met—no requirements met</div><div>Partly met—some requirements met</div><div>Mostly met—most requirements met</div><div>Met—all requirements met</div></div>			

Source: ANAO analysis.

2.4 The ANAO's review of the selected entities' implementation of the Commonwealth Policy indicated that specific matters which warrant further attention relate to:

- defining the entity's risk appetite in the risk management policy (ACMA);
- enhancing risk management capability (Health, AFMA and ACMA);
- improving the identification and management of shared risks (all entities);
- developing arrangements for communicating and consulting on risk with external stakeholders (all entities);
- improving arrangements to regularly review risks, risk management frameworks and the application of risk management practices (Health, AFMA and ACMA);
- seeking formal assurance from managers in preparing the responses to the Comcover survey of risk maturity (all entities);
- fully embedding the corporate plan requirement relating to risk (all entities); and
- assigning responsibility for risk management to individuals or positions, rather than work areas (Health, ACMA and AFMA).

2.5 To assess the selected entities' implementation of the overarching goal of the Commonwealth Policy<sup>27</sup> and its policy element five—developing a positive risk culture<sup>28</sup>—the ANAO had regard to: entities' implementation of the Commonwealth Policy requirements (summarised in Table 2.2 above); risk management in a selection of business activities in each entity; and the consideration of risk by senior leaders.

2.6 The ANAO's review of a selection of business activities<sup>29</sup> indicates that risk management informs normal business operations in the selected entities. Risk was considered when key business decisions were made or advice was provided to senior management or government by the areas selected for review. Further, the risk framework and key risks were regularly considered at senior levels within the selected entities (see paragraph 2.33).

2.7 In summary, the ANAO's review indicated that Employment has met, and Health and ACMA have mostly met, the requirement of policy element five and the overarching goal of the Commonwealth Policy. AFMA has partly met the requirement of policy element five and the overarching Policy goal.

2.8 The selected entities' implementation of the Commonwealth Risk Management Policy is discussed in more detail later in this chapter.

---

27 As discussed, paragraph 7 of the Commonwealth Policy states that 'The goal of the Commonwealth Risk Management Policy is to embed risk management as part of the culture of Commonwealth entities where the shared understanding of risk leads to well informed decision making.'

28 The Commonwealth Policy advises that risk culture is the set of shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities (paragraph 17). A positive risk culture: promotes an open and proactive approach to managing risk that considers both threat and opportunity; and is one where risk is appropriately identified, assessed, communicated and managed across all levels of the entity (paragraph 18).

29 Footnote 37 summarises the ANAO's methodology for assessing risk management at an operational level within the selected entities.



## Comcover Risk Management Benchmarking surveys

2.9 In 2015 and 2016, Comcover conducted a Risk Management Benchmarking survey that provided participating entities the opportunity to assess their level of maturity against each of the nine elements of the Commonwealth Risk Management Policy and to obtain an overall level of maturity based on their responses to the surveys. The six level risk maturity model is illustrated in Figure 2.1.

**Figure 2.1: Six level risk maturity model rating**



Source: Risk Management Benchmarking Program 2016: Comcover's *Key Findings Report*.

2.10 While entities' maturity levels and targets indicate where there remains scope for improvement in risk management capabilities, they are not a compliance rating. Accountable authorities are responsible for entity risk settings having regard to their business and operating environment. Maturity levels and targets may therefore differ between entities, and are not mandated.

## Selected entities' self-assessment

2.11 Table 2.3 presents the selected entities' self-assessment of their risk maturity levels against the nine elements of the Commonwealth Policy for 2016, and their target level of maturity for the following year.

**Table 2.3: Entities' 2016 self-assessment of their risk maturity levels, and targets for 2017, against the nine elements of the Commonwealth Policy.**

Elements in the Commonwealth Risk Management Policy		Entities' 2016 Self-Assessment of Risk Maturity Levels			
		Employment	Health	ACMA	AFMA
Element 1. Establishing a risk management policy	2016 Result	Optimal	Advanced	Advanced	Systematic
	2017 Target	Optimal	Integrated	Advanced	Advanced
Element 2. Establishing a risk management framework	2016 Result	Optimal	Integrated	Advanced*	Systematic
	2017 Target	Advanced	Integrated	Advanced	Advanced
Element 3. Defining responsibility for risk management	2016 Result	Optimal	Advanced	Integrated	Systematic
	2017 Target	Optimal	Integrated	Integrated	Integrated
Element 4. Embedding systematic risk management into business processes	2016 Result	Optimal	Integrated	Advanced	Systematic
	2017 Target	Advanced	Integrated	Advanced	Integrated
Element 5. Developing a positive risk culture	2016 Result	Optimal	Integrated	Advanced	Developed
	2017 Target	Advanced	Integrated	Advanced	Integrated

Elements in the Commonwealth Risk Management Policy	Entities' 2016 Self-Assessment of Risk Maturity Levels				
		Employment	Health	ACMA	AFMA
Element 6. Communicating and consulting about risk	2016 Result	Advanced	Systematic	Integrated	Systematic
	2017 Target	Optimal	Integrated	Advanced	Integrated
Element 7. Understanding and managing shared risk	2016 Result	Advanced*	Developed	Advanced*	Fundamental
	2017 Target	Advanced	Integrated	Advanced	Integrated
Element 8. Managing risk management capability	2016 Result	Advanced	Developed	Systematic	Developed
	2017 Target	Integrated	Integrated	Advanced	Integrated
Element 9. Reviewing and continuously improving the management of risk	2016 Result	Advanced	Integrated	Integrated	Systematic
	2017 Target	Advanced	Integrated	Advanced	Integrated

Note: \* Entities self-assessed as Advanced, while the ANAO's assessment was 'partly met'.

Source: Risk Management Benchmarking Program 2016: Comcover's Key Findings Report.

2.12 The ANAO's review indicates that there is broad alignment on the majority of elements between the ANAO's assessment of the selected entities' implementation of the Commonwealth Risk Management Policy (Table 2.2) and entities' 2016 self-assessment of their risk maturity levels (Table 2.3).<sup>30</sup>

2.13 As part of its review, the ANAO sought information to support the selected entities' responses to the 2016 survey.

2.14 Entities provided the ANAO with a range of documentation that supported the majority of their survey responses. To strengthen the level of assurance provided to senior leaders, entities could consider:

- improving the level of documentation they maintain in support of responses to future surveys; and
- obtaining formal management sign-offs to support entity responses to survey questions that relate to risk management practices in operational areas.

## Key Findings Report on 2016 Risk Management Benchmarking Survey

2.15 The Key Findings Report prepared for Comcover, following the 2016 Risk Management Benchmarking Survey, summarised the key observations relating to the self-assessment of 143 Australian Government (non-Corporate) entities. The report's key findings are in Box 4.

30 In three instances (\* in Table 2.3), entities self-assessed as *Advanced*, while the ANAO's assessment was *partly met*.

**Box 4: Summary of key findings from the 2016 benchmarking survey**

- The majority of entities' risk management policies include the core components [Element 1].
- Opportunities exist to expand risk identification techniques [Element 2].
- Limited use of key risk indicators in risk identification, analysis and reporting [Element 2].
- Key risk management roles and responsibilities are not often defined [Element 3].
- Few entities utilise a function to be solely or primarily responsible for risk management [Element 3].
- Unexpected performance around embedding systematic risk management into business processes [Element 4, 5 and 8].
- Few entities have regular processes for assessing risk culture [Element 5].
- Limited communication of risk information to external parties [Element 6 and 8].
- The highest proportion of entities scored a maturity of *Fundamental* [Element 7].
- Limited capability development and maintenance activities targeted to risk management [Element 8].
- Insufficient training is provided to some key risk management groups [Element 8].
- Measuring, assessing and reporting risk management performance [Element 9].

Source: Risk Management Benchmarking Program 2016: Comcover's Key Findings Report.

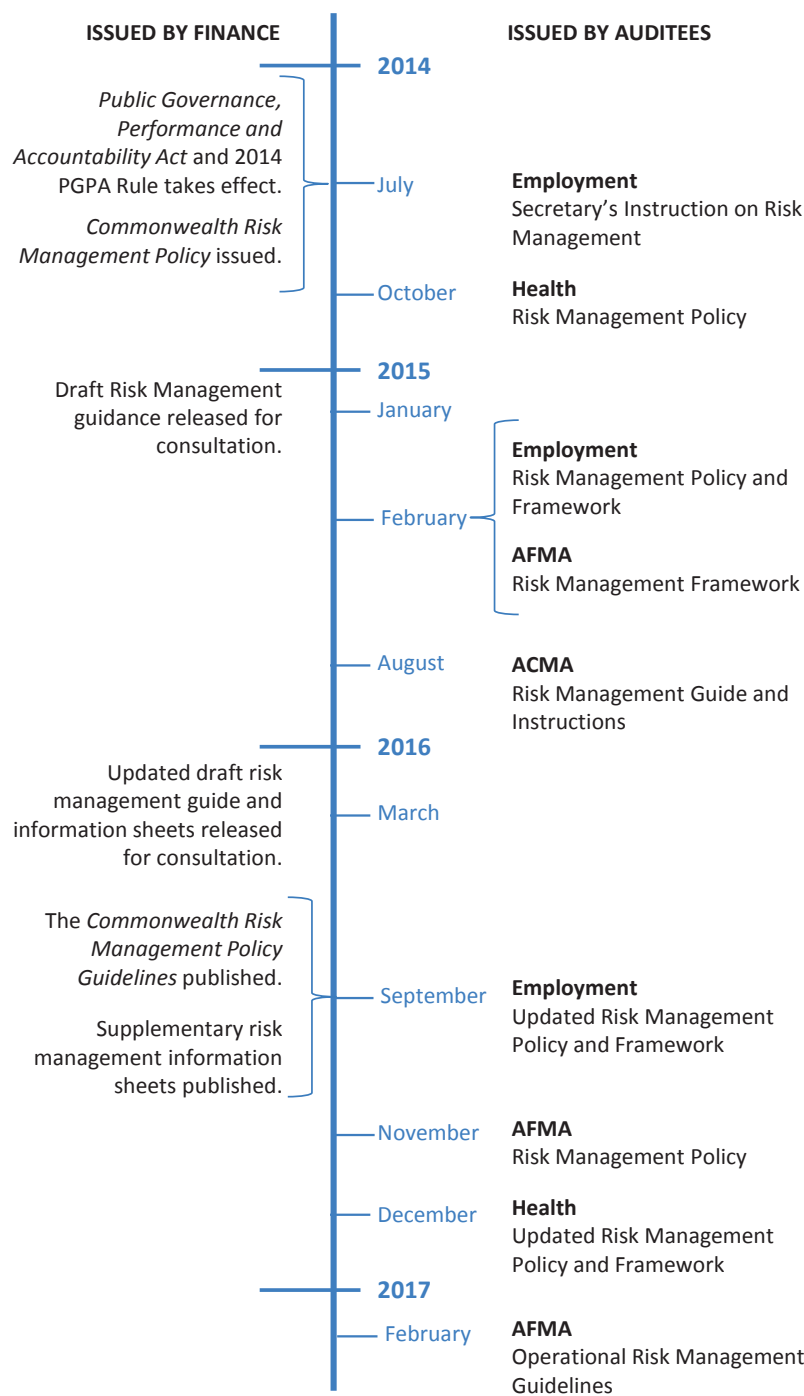
### **Did entities update their risk policy and framework in a timely manner following the issue of the Commonwealth Risk Management Policy?**

Each of the selected entities released an updated risk policy and framework within 12 months of the release of the Commonwealth Risk Management Policy. The selected entities have also continued to update elements of their policy and framework (Employment and AFMA) or have plans to do so (Health and ACMA).

2.16 As discussed, the Commonwealth Risk Management Policy was issued on 1 July 2014 by the Minister for Finance. Elements One and Two of the Commonwealth Policy require entities to establish a risk management policy and framework.

2.17 Key issue dates of entities' risk management policy and framework (Employment, Health and AFMA), guide and instructions (ACMA) are illustrated in Figure 2.2 and discussed in the following paragraphs.

**Figure 2.2: Issue dates of entities’ risk management policy and framework**



Source: ANAO analysis.

2.18 Each entity released an updated risk policy and framework within 12 months of the release of the Commonwealth Policy:

- Employment had issued its first departmental risk management policy and framework in December 2013. In July 2014—and in response to the release of the Commonwealth Policy—the department released a *Secretary's Instruction* on its risk management policy and framework. The department updated its 2013 risk management policy and framework in February 2015. This update reflected the department's most recent thinking around risk appetite and tolerance. The department had identified that the application of the risk matrix released in 2013 was resulting in some risks being rated as 'high' that were not significant risks. In September 2016, the risk policy and framework were revised further to include a detailed *Risk Appetite Statement*.
- Health issued a revised departmental risk management policy and framework in October 2014, three months after the release of the Commonwealth Policy. The department's 2014 risk management policy states that the policy should be reviewed and updated annually.<sup>31</sup> In December 2016, Health released a new Risk Appetite following extensive internal consultation.
- ACMA issued a revised risk management guide and management instruction in July 2015, 12 months after the release of the Commonwealth Policy. ACMA's 2015 risk management guidance states that the policy should be reviewed and updated annually. The guide was due to be reviewed in the second half of 2016. ACMA advised the ANAO that it has decided to await the outcomes of this audit before finalising its review.
- AFMA issued a revised risk management framework in February 2015, seven months after the release of the Commonwealth Policy. AFMA's 2013 risk management framework states that the framework should be reviewed in February and August each year. The authority released an updated risk management policy, which included a risk appetite statement, in November 2016. AFMA issued risk management operational guidelines in February 2017.

2.19 Elements One and Two of the Commonwealth Policy have a number of additional detailed requirements which overlap to some extent with other elements of the Commonwealth Policy. These requirements relate to building a risk management framework and culture and include:

- internal and external consultations;
- embedding risk management into business processes;
- managing shared risks; and
- reviewing and improving the risk management framework.

2.20 The application of these specific requirements is discussed in the remainder of this chapter in the context of the relevant element.

---

31 Health advised the ANAO that the next review and update is scheduled for early 2017.

## Are entities' risk management frameworks developed with relevant stakeholder consultation, including arrangements to consult in a timely and effective manner?

The selected entities' risk management frameworks were developed with extensive internal consultation, including with audit committees. There remains scope for entities to include, in their risk framework documentation, their arrangements for communicating, consulting and reporting on risk to both their internal and external stakeholders.

2.21 An entity's risk management framework is required to include how the entity will report risks to both internal and external stakeholders. Each entity must also implement arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders (See Elements Two and Six of the Commonwealth Policy).

2.22 Each of the selected entities' frameworks was developed with extensive internal consultation, including with entities' audit committees<sup>32</sup>, although entity frameworks do not explicitly outline arrangements for communicating and consulting about risk with internal and external stakeholders. None of the selected entities outlined arrangements for reporting on risk to stakeholders. Entities advised the ANAO that in practice consultation on risk occurs as part of the routine consultation and interaction with external stakeholders (for all entities), research and scientific expert groups (ACMA and AFMA) and other Commonwealth entities (for all entities).

2.23 There is scope for entity frameworks to outline arrangements for communicating, consulting and reporting on risk to internal and external stakeholders (all entities). These arrangements could be considered as part of the regular review of an entity's risk policy and framework.

## Are responsibilities and accountabilities for risk management clearly defined?

For three entities, responsibilities for managing and reporting on risk are clearly identified (Employment, Health and AFMA). ACMA has documented some, but not all, responsibilities.

2.24 The Commonwealth Policy requires that responsibilities for managing risk be defined within an entity's risk management policy (see Elements One and Three of the Commonwealth Policy).

2.25 For Employment, Health and AFMA, the responsibilities for managing and reporting on risk are clearly outlined as part of their risk management framework. Their risk frameworks address key responsibilities relating to:

- the review and update of the risk management policy and framework, and individual risk plans and risk treatments; and

32 The PGPA Rule 2014 provides that the functions of an entity's audit committee must include reviewing the appropriateness of the accountable authority's system of risk oversight and control. The ANAO survey of the PGPA Rule is discussed in Audit Report No.33 2016–17 *Financial Statement Audit*.

- descriptions of key positions, including senior executives, program/policy/project managers and risk owners; department committees (such as the Executive Committee and the Audit Committee); and business areas.

2.26 The responsibilities for managing and reporting on departmental risks are less well defined for ACMA. ACMA had documented specific expectations of some of its executive and senior management staff, including for the review of risk registers and controls. There would also be benefit in defining the responsibilities of the Governance Board and its supporting committees, and the Strategic Risk and Planning Section.

2.27 Each of the selected entities' risk management frameworks provide that responsibility for risk plans, individual risks and risk treatments should be assigned to an individual person or position. This approach is consistent with the *Australian/New Zealand Standard Risk Management—principles and guidelines*. In practice there was variability in the application of this approach within some entities, and responsibilities were often assigned to work areas. Entities should consistently assign responsibility to individuals or positions, in line with the requirement of their frameworks (Health, ACMA and AFMA).

## Are entities' risk appetite and risk tolerance defined?

Three of the selected entities developed new or revised risk appetite and tolerance statements following the release of the Commonwealth Policy (Employment, Health and AFMA). One entity included a risk tolerance statement in its 2015 risk management guide, but has not developed a risk appetite statement (ACMA).

2.28 The Commonwealth Policy requires that entities define their risk appetite and tolerance (see Element One).<sup>33</sup> According to Comcover, the development of a risk appetite statement that incorporates risk tolerances that are tailored to an entity's particular circumstances would be an important milestone in enhancing an entity's risk management framework.<sup>34</sup> The statement would: provide a platform to assist in making informed decisions; provide the potential for consistent risk management practices; and help to guide discussions on risks and risk treatments.<sup>35</sup>

2.29 Documenting an entity's risk appetite and tolerance is a necessary first step to developing a risk framework that reflects the entity's particular circumstances and which can directly assist in decision making.

2.30 Employment, Health and AFMA have developed new or revised risk appetite and tolerance statements as a key element of their respective risk management frameworks introduced following the release of the Commonwealth Policy.

33 According to the Commonwealth Policy (p. 21), *risk appetite* is the amount of risk an entity is willing to accept or retain to achieve its objectives—it is a statement or series of statements that describes the entity's attitude toward risk taking. *Risk tolerance* is defined as the levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk.

34 Department of Finance, *Information Sheet: Defining Risk Appetite and Tolerance*, Finance, 2016.

35 *ibid.*

- Employment's current risk management policy and framework were issued in September 2016. A revised risk appetite statement was a key element of the framework, and includes risk tolerances for a range of risk categories and sub-categories. The statement is readily accessible from the department's Intranet.
- Health conducted a review of its risk appetite and risk tolerance from October 2014 to late 2016, and released an updated risk appetite statement in December 2016. The updated risk appetite statement classifies risks against seven risk themes: people, fraud, policy, delivery, governance, regulatory and information. Health's enterprise-level risks have been updated and are aligned with the seven risk themes (see Appendix 4 for Health's enterprise risk appetite statement).
- AFMA released an updated risk management policy in November 2016 which included its risk appetite and risk tolerance statements. AFMA's policy describes five ascending levels of appetite: averse; minimal; cautious; open; and hungry. According to AFMA's risk policy, 'AFMA is generally open to risk, in that it is willing to consider all options and choose the one most likely to result in successful delivery while also providing an acceptable level of reward and value for money.' However, within this broad approach, a number of key risk areas have different risk appetites.

#### Good practice example 1. Employment's and Health's risk appetite statements

The development of Employment's 2015 risk appetite statement involved extensive internal consultation and was funded, in part, by the Department of Finance (Comcover) as a pilot with the objective of using the statement as an example of good practice to assist other entities develop their own statements. Comcover considered the project would benefit other entities, and has published a case study featuring the department's statement, accessible from Comcover's website.<sup>a</sup>

Health's risk appetite statement is illustrated at Appendix 4. The statement is presented as an infographic on one page for ease of reference. It includes information on the enterprise risk appetite, risk themes and scaling, and supporting a risk aware culture. It is effective in communicating expectations to departmental staff.

Note a: Available at <<http://www.finance.gov.au/comcover/policy/resources.html>> [Accessed 28 February 2017].

2.31 ACMA included a risk tolerance statement in its 2015 risk management guide, but has not developed a risk appetite statement. ACMA's risk tolerance statement is adopted from the *Work Health and Safety Act 2011* and details the principle of managing risks to a level that is 'as low as reasonably practicable' (ALARP).<sup>36</sup>

36 Managing risks to an ALARP-level is one of the fundamental principles of health and safety management, and the term 'reasonably practicable' is used in the *Work Health and Safety Act 2011* (Subdivision 2, Section 18) and the *Work Health and Safety Regulations 2011* (Part 3.1, section 35).



## Is risk considered as part of key business decisions and operations?

The risk framework and key risks were regularly considered at senior levels within the selected entities. There is scope for a more structured approach to reporting on and reviewing enterprise-level risks and the status of risk controls and treatments (Health and AFMA). As discussed at paragraph 2.42, at present there is limited management reporting to the Executive Committee (Health) or Commission (AFMA) on enterprise-level risks, and no reporting on operational risks to the Audit and Risk Committee (Health and AFMA).

The ANAO's review of a selection of business activities in each entity indicates that risk management also informs normal business operations. Risk was considered when key business decisions were made or advice was provided to senior management or government in the areas selected for review.

2.32 The Commonwealth Policy requires that each entity must ensure that the systematic management of risk is embedded in key business processes (Element 4).

2.33 The risk framework and key risks were regularly considered at senior levels within the selected entities—including the executive committee (Employment and Health), senior executive (ACMA) and the Commission (AFMA). Further, the ANAO's review of a selection of business activities in each entity indicated that their activities were informed by considerations of risk. Risk was considered when key business decisions were made or advice was provided to senior management or government by the areas selected for review.<sup>37</sup>

- Employment's Risk and Implementation Committee (ERIC) met six times each year in 2014, 2015 and 2016 to consider and oversight the operations of the department's risk management policy and framework, and reported quarterly to the department's executive committee on the adequacy of the risk framework and associated processes. Following a 2016 review of governance committees, ERIC was disbanded in December 2016 and the Finance and Business Services Committee (FABS) was given responsibility to advise the Secretary on: risks identified in relation to the department's ability to meet its business goals, as per the Risk Management Framework; and work to improve the department's risk and policy framework, and lead the application of risk management across the department. At its meeting in March 2017, the FABS: noted that the department's Executive had participated in a workshop to review entity strategic risks in February 2017; and considered an entity-level risk monitoring report. The department's *Performance and Integrity Sub Committee for Employment Services* (PISCES) provides a high-level forum to support and advise on maximising the performance and integrity of all contracted

37 To assess risk management at an operational level, the ANAO reviewed risk management in selected divisions of Employment, Health and ACMA. The selected divisions had the highest number of risks and/or the highest severity of risks recorded in the entities' enterprise risk register. The selected divisions were: Workers Compensation Policy Branch, and Job Seekers Compliance Section (Employment); The Office of the Gene Technology Regulator, Health Provider Compliance Division, and Population Health and Sports Division (Health); and Content, Consumer and Citizen Division (ACMA). AFMA has only three branches—Corporate, Fisheries Management and Fisheries Operations. The ANAO selected the Fisheries Management Branch for review on the basis of the highest identified risks in the risk register.

employment services under jobactive.<sup>38</sup> The department's Audit Committee also regularly receives updates from management on aspects of the department's risk framework and obtains presentations from time to time from responsible departmental managers on the management of risks in respect of specific programs or activities. The operational divisions reviewed by the ANAO employed the department's enterprise-wide risk management system (RiskActive) to assist in managing risk.<sup>39</sup>

- Key risks were regularly considered by Health's executive committee in its consideration of specific departmental strategies and plans. There is scope for a more structured approach to reporting on and reviewing enterprise-level risks and the status of risk controls and treatments. The three operational divisions examined by the ANAO had established a range of local mechanisms to monitor, report on and manage risk.
- ACMA's key risks were reviewed quarterly by the senior executive as part of a regular cycle. Staff were also able to show that an assessment of risk informed local decision making processes, and that risk conversations at the senior and middle management levels took place. At an operational level, delegations for decision making relating to broadcasting and datacasting investigations were based on the assessed level of risk of each investigation.
- Sustainability risks were regularly considered by the AFMA Commission in its consideration of specific fisheries management strategies and plans. Available records indicated that the operational branch selected for review had produced a range of risk assessments and guidance on risk management. There is scope for a more structured approach to reporting on and reviewing enterprise-level risks, controls and treatments.

#### **Good practice example 2. De-prioritise and de-fund low-level activities**

The Australian Communications and Media Authority's senior executive decided in May 2016 to adopt a risk-based approach to resource allocation for the 2016–17 financial year. The Authority's division and branch heads were asked to identify potential activities and to rate the risk of removing those activities. Items that were rated as 'low risk' were accepted and removed from ACMA's activities, resulting in savings of \$1.998 million across ACMA.

2.34 The ANAO's review of the selected entities' records, and discussions with a range of officials, indicated that project and program risks are routinely discussed at regular management and work place meetings, and with other entities and contracted service providers, although records of such operational meetings are often not maintained by entities.

38 Which include Work for Dole, New Enterprise Incentive Scheme (NEIS), Harvest Labour Services and the Harvest Labour Information Service and Work for the Dole Coordinators.

39 The system is discussed further in paragraph 2.45 of this audit report.

**Good practice example 3: Conducting risk premortems**

The Department of Employment promotes the use of risk premortems as a way for work areas to identify and openly discuss risks to a new project or activity. A premortem begins with the assumption that a project has been implemented and the project has failed. The work group then identifies the reasons for the failure. In this way the group is able to constructively focus on the key risks involved in meeting the objectives of a program or activity. Conducting risk premortems is also a simple way to openly discuss causes of failure, without ascribing blame. It allows more junior officers and people familiar with differing facets of a project to voice their concerns in a non-judgemental forum.

**Have entities established arrangements to manage shared risks?**

The identification and management of shared risks is one of the least mature elements of entities' implementation of the Commonwealth Policy. Shared risks are not routinely identified and managed as such in the context of entities' risk management policies and frameworks (Health, ACMA and AFMA).

2.35 The Commonwealth Policy provides that an entity must establish a risk management framework which includes how the entity contributes to managing any shared or cross-jurisdictional risks, and must implement arrangements to understand and contribute to the management of shared risks (Elements Two and Seven).

2.36 The Commonwealth Policy defines a shared risk as a risk with no single owner, where more than one entity is exposed to or can significantly influence the risk.<sup>40</sup> Shared risks are those extending beyond a single entity, which require shared oversight and management. Accountability and responsibility for the management of shared risks should include any risks that extend across entities and may involve other sectors, the community, industry or other jurisdictions.<sup>41</sup>

2.37 The Comcover 2016 Benchmarking Survey noted that understanding how to identify what is a shared risk is a concept that entities find challenging. Understanding and managing shared risk is important for effective policy and program design and implementation.

2.38 A useful starting point in considering shared risk is to focus on shared outcome risks, rather than low-level transactional risks. A risk management strategy can usefully identify areas where an entity is reliant on others to achieve its outcomes, or whose actions and activities will impact on the achievement of entity outcomes.

2.39 Entities have in place arrangements, such as steering and consultative committees, which contribute to managing risks that relate to programs and activities which involve other entities or external parties. These risks are not routinely identified and managed as shared risks in the context of entities' risk management policies and frameworks.

40 Department of Finance, *Commonwealth Risk Management Policy*, July 2014, p. 21.

41 *ibid.*, paragraph 20.

- Employment did not routinely categorise and manage shared risks other than risks relating to the Shared Services Centre.<sup>42</sup> It is not evident that other risks are recognised in departmental risk registers and managed as shared risks, and risk reporting does not include reporting on shared risks.
- Health’s risk management policy defines shared risks and the department’s risk register templates make provision for recording them. The ANAO’s review identified that some of the assigned shared risks were intra-entity—such as risks shared with other areas of the department—whereas the Commonwealth Policy defines a shared risk as one extending beyond the entity.
- ACMA does not refer to shared risk in its risk guidance and instruction, and there is no explanation of how shared risks should be identified and managed. In practice, ACMA and its portfolio department have created a shared risk register for their joint steering committee. ACMA advised the ANAO that arrangements for identifying and managing shared risks will be developed as part of a planned review of the risk framework.
- AFMA is in the early stages of implementing its risk guidelines and its approach to external consultation and shared risks. AFMA’s 2017 risk management guidelines addressed the issue of establishing shared risks through external consultation processes:

External consultation will establish shared risks through engagement with other Commonwealth agencies, cross-jurisdictional entities, industry and interest groups. Once every 12 months AFMA’s Risk Manager will engage with external stakeholders to establish the register of shared risks and report the findings to the Audit and Risk Committee and the AFMA Commission.

## Do entities have relevant capability to underpin the management of risk?

The selected entities have implemented a range of measures to build their risk management capability. Key measures include:

- regular internal reporting on the entity’s risk profile and risk framework (Employment and ACMA);
- risk management guidance, templates and dedicated risk hot lines or email addresses (Employment, Health and ACMA);
- staff resources dedicated to risk management (Employment, Health);
- custom-built risk management systems (Employment); and
- learning and development programs which address risk management, including eLearning modules (Employment, Health and ACMA).

42 The Shared Services Centre (SSC) was administered jointly by the Department of Employment, and the Department of Education and Training (Education) and provided a variety of services to each department and other government entities. As part of machinery of government changes in September 2016, some functions moved to the Finance portfolio, such as governance arrangements for joint services.

2.40 The Commonwealth Risk Management Policy provides that entities must maintain an appropriate level of capability to both implement the entity's risk management framework and manage its risks (Element Eight).

2.41 The ANAO reviewed the following aspects of the selected entities' risk management capability:

- governance and reporting arrangements;
- supporting guidance, systems and processes; and
- learning and development programs, individual performance development, and awards and incentives.

### **Governance and reporting arrangements**

2.42 The risk management policies developed by Employment, Health and AFMA outline governance arrangements for risk management, including a summary of key roles and responsibilities for internal committees and individual management positions with risk responsibilities. At the time of the audit, there was:

- limited management reporting to the executive committee (Health) or Commission (AFMA) on the status of enterprise-level risks, as part of a structured process of regular review of enterprise-level risks, controls and treatments; and
- no reporting of operational (division-level) risks to the Audit and Risk Committee, including the status of risk controls and treatments (Health and AFMA).<sup>43 44</sup>

2.43 ACMA's Executive Group receives a quarterly report on risk management. These reports discuss current risks and emerging risks and risks that have been retired and removed. These reports also provide an update on risk metrics (such as the number of risks and the level of risks) and a summary of other relevant information. Divisional reports on the operation of the risk management framework and processes are also submitted to the Audit Committee every quarter.

2.44 Employment records indicate that risks, risk plans and risk treatments are actively managed by risk owners, and there is regular reporting to the senior executive and audit committee on the status of risks and risk treatments.<sup>45</sup>

### **Supporting guidance, systems and processes**

2.45 Employment has placed extensive risk management guidance on its Intranet to assist staff to manage risks and risk treatments. The department operates and maintains an integrated, enterprise-wide risk management systems to assist in managing its risks—*RiskActive*. The system

43 In the absence of consolidated reporting on risk, Health's Audit and Risk Committee relies on *ad hoc* presentations from Branch and Division-level representatives on their risk management.

44 AFMA has developed a work plan for an enterprise risk register. The authority advised the ANAO in June 2017 that a working model of the enterprise risk register and risk reports was reviewed by the Executive, Audit and Risk Committee on 6 June 2017, and is scheduled for review by the AFMA Commission on 28 June.

45 The ANAO's review also indicated that the detailed risk treatments in risk plans (as recorded in *RiskActive*) are used to determine the allocation of resources.

is mature and provides the department with the capability to record, manage and report on risks, risk treatments, risk events and risk plan owners.<sup>46</sup>

2.46 Health requires that risk registers should be used by operational divisions to identify and classify risks, and to list controls and risk treatments. Health does not have in place arrangements to provide assurance that risk registers are regularly reviewed in accordance with the department's risk management policy.

2.47 ACMA's risk management guidance provides a high-level description of risk management, but limited practical guidance on how staff should manage risk. ACMA has a formal process for divisions to identify, manage and report risks. Templates are provided to the divisions, and support is provided when required to assist with the process.

2.48 Risk management guidance available on AFMA's Intranet was minimal and not up to date.<sup>47</sup> This is an impediment to the development of a positive risk management culture. Other risk-related guidance available on the Intranet focussed on project management, and did not include guidance for business as usual activities. Project management templates, including a register, were available to identify, monitor and report on project risks.

## Learning and development

2.49 Employment's learning and development program includes offerings on risk management including a number of risk management eLearning modules.<sup>48</sup> Departmental officials are regular participants in risk management forums and seminars organised by Comcover and departmental officials are encouraged to attend and participate in external risk management seminars and courses. Risk management is also identified as one of the criteria used to judge the recipients of the Secretary's award for innovation.

2.50 Health and ACMA have a variety of learning and development programs available for staff, including eLearning courses developed by Comcover and entity-specific workshops.

- Health held a variety of Comcover Risk workshops for its senior executives on risk, controls and shared risk in 2016 and 2017. Health also introduced an e-learning module in January 2017, but there has been limited uptake of this training module<sup>49</sup>; and
- 79 per cent of ACMA employees had completed the compulsory risk management e-learning module in 2016 with plans to add risk-specific guidance to its induction program.

2.51 AFMA does not have formal learning and development programs in risk management for staff, a further impediment to the development of a positive risk management culture. The ANAO

---

46 As at December 2016, departmental systems included 540 risk plans, 2558 risks, 6806 risk treatments and 242 risk plan owners.

47 In December 2016 AFMA's Intranet included links to its Risk Management Framework 2013 document and Chief Executive Instructions. AFMA advised the ANAO in February 2017 that revised guidance had not yet been released internally.

48 Of a total of over 1950 Employment staff (at 30 June 2016)—240 staff had accessed the eLearning module, *Risk Essentials*. Of these, 213 were recorded as having 'passed' the module. Fifty-three staff were recorded as having accessed the eLearning module, *RiskActive*.

49 Of a total of over 5000 Health staff (at 30 June 2016)—32 staff had completed the e-learning module, and 29 staff had attended a risk management workshop.

was advised by AFMA that work had commenced to implement a training package for staff on the *Public Governance, Performance and Accountability (PGPA) Act 2013*, including a risk management module.<sup>50</sup>

## Are entities' risk management frameworks reviewed to continuously improve the management of risks?

The selected entities' risk management policies include a commitment to regularly review the risk framework, and each of the entities has continued to review its risk management policies and framework since the Commonwealth Policy was released in July 2014.

2.52 The Commonwealth Policy provides that each entity must review its risks, its risk management framework and the application of its risk management practices on a regular basis, and implement improvements arising out of such reviews (see Element Nine).

### Review

2.53 The selected entities' risk management policies include a commitment to regularly review the risk framework.

- As discussed in paragraph 2.18, Employment has twice revised or updated its risk policy since 2014 (in 2015 and 2016).
- Aspects of Health's risk management were reviewed as part of the 2014 Health Capability Review, which observed that the department needed to foster a culture that appropriately embraces and manages risks within agreed tolerances.<sup>51</sup> In response, the department initiated a review of the risk management component of the Health Capability Program in July 2016. The 2016 review commented that more work needed to be done. The department has an ongoing program to address the recommendations of the two reviews. A key focus of the capability program is to fully operationalise the department's risk management framework.
- As discussed in paragraph 2.43, ACMA has established processes for executive review of division-level risks and conducted reviews of its risk registers in 2015 and 2016;
- AFMA conducted a review of the authority's risk management framework in June 2015, and has implemented or partially implemented seven of the ten recommendations arising from the review (at February 2017).

2.54 Regular review of entities' risk frameworks and practices improves the effectiveness of risk management, and should be factored into internal planning processes.

50 At the time of the audit, Learnhub was being implemented as an e-learning tool that provided a range of courses across the APS, including the *Introduction to Risk in the Commonwealth*. The course is sponsored and maintained by Comcover and is designed to increase awareness of risk across the Commonwealth Public Sector and encourage better practice in public sector risk management.

51 Australian Public Service Commission, *Capability Review: Department of Health*, October 2014, p. 12.

## Escalating and recording issues

2.55 The selected entities did not systematically record and analyse risk incidents, issues and events to inform their periodic evaluation of the risk management framework, and there was variability in processes for escalating risk.

- Employment has developed a process for the escalation of high and extreme risks. Departmental staff interviewed by the ANAO indicated that in their experience, senior management adopted a supportive and constructive approach when risk events and incidents are reported. Departmental procedures include a requirement for 'plan events' to be recorded in *RiskActive* and for such events to trigger a review of the relevant Risk Plan. The guidance outlines detailed actions to be taken depending on whether the event was, or was not, previously identified as a risk.<sup>52</sup> The ANAO's review of a selection of risk events indicates that a number of the events recorded are events or developments that have occurred but are not related to the risks or risk treatments outlined in the relevant risk plan and it was not evident that risk events routinely triggered a review of the risk plan.
- Health has limited guidance in the risk template which advises staff on the escalation of high and extreme risks. Departmental staff interviewed by the ANAO indicated that in their experience the attitude to reporting and escalating risks has improved significantly in the past two years, and the focus is now on identifying issues, finding solutions and learning lessons from the risk events.
- The ANAO was advised by ACMA that it is developing a new risk escalation process. ACMA does not record risk incidents to assist in monitoring the adequacy of its risk framework. However, some of the ACMA End Project Reports reviewed by the ANAO identified project risks and noted whether the risks materialised or not.
- AFMA's risk guidance documented a pathway for the annual review and escalation of risks, but did not provide guidance for the escalation of high and extreme risks as they emerged. AFMA employees interviewed by the ANAO indicated that reporting on risks occurred on a case-by-case basis, and as needed.

2.56 Recording and analysing risk incidents and lessons learned can provide valuable insights to management and the audit committee on risk management performance and the effectiveness of the risk management framework.

---

52 The ANAO's sample review of *RiskActive* identified that 78 risk events were recorded against 40 risk plans at the time of audit.



## Reporting on risk management performance

2.57 The selected entities do not have mechanisms in place to measure risk management performance:

- Employment's records do not indicate that the department assesses and reports on the performance of the risk management framework in accordance with the approach outlined in the risk management policy.<sup>53</sup>
- Health, ACMA and AFMA advised the ANAO that they rely on the results from the annual Comcover Benchmarking survey to assess the performance of their risk management frameworks. With the exception of this survey, these entities do not have any mechanisms in place to measure risk management performance.<sup>54</sup>

## Other reporting on risk management performance

2.58 The Australian Public Service Commission (APSC) surveys APS agencies and employees annually on a range of workforce management issues. Both surveys have included a number of questions relating to risk management. The 2016 APS employee census included four questions relating to entities' risk management.

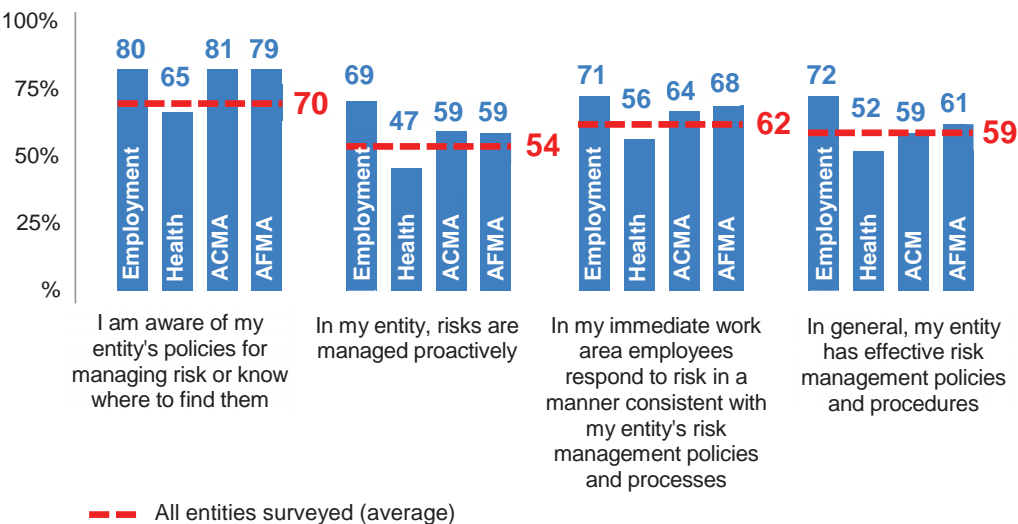
2.59 Figure 2.3 presents the survey results for the selected entities (blue) compared to the results for all agencies surveyed (red). This analysis indicates that a higher proportion of employees in Employment, ACMA and AFMA agreed with the risk-related statements in the 2016 survey, when compared with the combined results for all entities surveyed. A lower proportion of Health employees agreed with those statements.

---

53 The department's risk management policy states that the performance of the risk management framework is assessed against the achievement of four objectives: organisational resilience; positive risk culture; integrated and consistent application; and informed and effective decision making. The department advised the ANAO in July 2017 that it has commenced planning for a review against the approach outlined in the policy, and has made reference to the relevant objectives in regular risk reporting.

54 Further, ACMA has not described performance measures for its risks or controls, as outlined in its risk management guidance.

**Figure 2.3: Staff responses to the risk-related questions in the 2016 APS employee census, compared to the overall score for all entities surveyed**



Source: ANAO analysis of data provided by the APSC.

2.60 The relatively high level of agreement indicated by Employment staff to the four questions is consistent with the department’s implementation of an integrated risk management system across the department, as reported in this audit. The relatively low level of agreement indicated by Health staff is consistent with that department’s state-of-play in fully operationalising its risk framework across the department, as reported in this audit.

2.61 All the selected entities (Employment, Health, ACMA and AFMA) advised the ANAO that the data provided by the APSC is not used in a substantive sense as part of management reporting and/or to assist in the review of their enterprise risk management framework.

2.62 Health also conducts a *Pulse Survey* every six months, which aims to complement the annual APSC survey. A summary of relevant results is presented in Table 2.4.

**Table 2.4: Results for the risk-related question in Health’s 2016 pulse surveys**

Question: In my branch, there is a willingness to take appropriate risks with decisions			
Survey date	Disagree (per cent)	Mixed (per cent)	Agree (per cent)
March 2016	26	32	42
October 2016	21	29	50

Source: ANAO, drawing on Department of Health records.

## Was risk addressed in entity corporate plans?

The selected entities were at different levels of maturity in their implementation of the corporate plan requirement relating to risk, with further work required in all entities to fully embed the requirement.

2.63 The PGPA Rule requires entity corporate plans to include a summary of the risk oversight and management systems of the entity for each reporting period covered by the plan (including the measures that will be implemented to ensure compliance with the finance law).

2.64 The 2016 Finance Guidance noted that:

As a strategic planning document, the corporate plan needs to demonstrate that effective systems of risk oversight and management have been implemented. Entities should explain how their approach to managing risk will support the achievement of their purposes.<sup>55</sup>

2.65 The 2017 Finance Guidance similarly noted that:

Entities should explain how risk management will underpin their approach to achieving their purposes... As a strategic planning document, the corporate plan should demonstrate that effective risk management priorities have been considered and implemented.<sup>56</sup>

2.66 As part of the audit, the ANAO assessed the maturity of the risk oversight and management section of the selected entities' 2016–17 corporate plans using the methodology used in the ANAO's Report No.6 (2016–17) *Corporate Planning in the Australian Public Sector* and Report No.54 (2016–17) *Corporate Planning in the Australian Public Sector*.













2.67 The ANAO's assessment of the maturity of the risk oversight and management section of the selected entities' 2016–17 corporate plan is presented in Table 2.5.

---

55 Department of Finance, *Resource Management Guide No. 132 - Corporate plans for Commonwealth entities*, Finance, July 2016, paragraph 79.

56 Department of Finance, *Resource Management Guide No. 132 - Corporate plans for Commonwealth entities*, Finance, January 2017, paragraph 83.

**Table 2.5: Assessment of the maturity of the risk oversight and management section of the selected entities' 2016–17 corporate plan**

Risk oversight and management					
<b>Department of Employment</b> The discussion of risk is generally at a high level and it is difficult to directly link the discussion to the department's purposes. The environment section of the plan includes some commentary on risk including five 'consequence families that represent the department's key areas of concern should risks occur'.					
<b>Department of Health</b> The discussion of risk mainly outlines how the department intends to improve its risk management framework. The risk section does not link to the department's purpose but does outline at a high level a governance structure that the plan suggests 'enables consideration of risk in all core business decisions'. The plan does not identify risk categories or specific risks.					
<b>ACMA</b> The discussion of risk addresses three main risks—ecological risks, compliance risks and operational risks—and summarises the Authority's risk framework and governance arrangements. The plan also provides internet links to more detailed documents available from the Authority's website. On its face, the plan is reasonably mature; the issue is that some of the information referred to is not supported by evidence. In particular, risk management plans were not evident and the Risk Management Committee did not meet for over two years.					
<b>AFMA</b> The discussion of risk includes a summary of the seven strategic risks facing the Authority, summarises the governance arrangements for the management of risk, and briefly outlines the Authority's risk tolerance and its approach to the assessment of risk.					
<b>Key</b> <div>  The discussion of risk does not address how the entity's approach to managing risk will support the achievement of the entity's purposes. </div> <div>  The discussion of risk is linked to the achievement of an entity's purposes but does not outline the sources of risk or the key risks that impact the achievement of an entity's purposes. </div>		<div>  The discussion of risk does not clearly address how the entity's approach to managing risk will support the achievement of the entity's purposes. </div> <div>  The discussion of risk is linked to the achievement of an entity's purposes and outlines the sources of risk or the key risks that impact the achievement of an entity's purposes. </div>			

Source: ANAO analysis.

2.68 The selected entities were at different levels of maturity in their implementation of the corporate plan requirement relating to risk, with further work required in all entities to fully embed the requirement. There would be benefit in the selected entities reviewing the Department of Finance's guidance on preparing corporate plans, which indicates that a mature approach to addressing risk in the corporate plan may include a discussion of:

- how the key sources of risk to an entity's purposes are being managed in the context in which the entity operates, the activities undertaken and the purposes the entity seeks to achieve;
- the capability and environment components of the corporate plan, and how those components impact the risk profile of the entity;
- key sources of emerging risks that may impact its ability to achieve its purposes in the future; and
- the risks an entity faces in the context in which the entity operates, the activities undertaken and the purposes it seeks to achieve.<sup>57 58</sup>

## Areas for improvement

2.69 The ANAO has not made any recommendations in this audit, but has highlighted a range of matters relating to the audited entities' risk management which warrant further attention. The matters highlighted below may also warrant attention by other Commonwealth entities.

2.70 Specific matters which warrant further attention by the selected entities relate to:

- defining the entity's risk appetite in the risk management policy (ACMA);
- enhancing risk management capability (Health, ACMA and AFMA);
- improving the identification and management of shared risks (all entities);
- developing arrangements for communicating, consulting and reporting on risk with internal and external stakeholders (all entities);
- improving arrangements to regularly review risks, risk management frameworks and the application of risk management practices (Health, ACMA and AFMA);
- seeking formal assurance from managers in preparing responses to the Comcover survey of risk maturity (all entities);
- fully embedding the corporate plan requirement relating to risk (all entities); and
- assigning responsibility for risk management to individuals or positions, rather than work areas (Health, ACMA and AFMA).



Grant Hehir  
Auditor-General

Canberra ACT  
15 August 2017

---

57 Department of Finance, *Resource Management Guide No. 132 - Corporate plans for Commonwealth entities*, Finance, July 2016, paragraphs 80 to 83.

58 The Department of Employment advised the ANAO in July 2017 that during the preparation of its 2017-18 corporate plan it had undertaken work to further embed the corporate plan requirement relating to risk, and had received positive feedback on draft content provided to the Department of Finance for comment.



# Appendices

## Appendix 1 Responses from the selected entities



Australian Government  
Department of Employment

Your Ref  
Our Ref 2017-00516

Acting Secretary  
Martin Hehir

Grant Hehir  
Auditor-General  
Australian National Audit Office  
GPO Box 707  
Canberra ACT 2601

Dear Mr Hehir

*Grant*  
The Department of Employment (the Department) welcomes the overall findings of the Australian National Audit Office's (the ANAO) Performance Audit of the Management of Risk by Public Sector Entities (the audit).

The Department recognises risk management is a cornerstone of good corporate governance and organisational success. Managing risk well enables us to achieve our outcomes and promotes the efficient, effective and ethical use of Australian Government resources. The audit concludes the Department has a mature and integrated approach to the identification and management of risk and has implemented a range of measures to build its risk capability. The Department has consciously invested in its risk management framework and I am pleased the ANAO has identified the positive returns from this investment.

The process of mature risk management is ongoing and we will take action in relation to areas for improvement identified in the audit that relate to the Department. The Department will examine its arrangements for communicating, consulting and reporting on risk with external stakeholders, and focus on better identifying and managing shared risk. The Department will continue to improve the presentation of its risk approach in its corporate plans, and will ensure appropriate assurances from relevant managers in preparing responses to the annual Comcover self-assessment of risk maturity.

The Department acknowledges the difference between the audit which assesses agency compliance and the Comcover survey which assesses agency maturity. Noting the disparities between auditees' Comcover survey maturity ratings and the ANAO's compliance ratings,

GPO Box 9880, Canberra ACT 2601 | Phone 1300 488 064 | [www.employment.gov.au](http://www.employment.gov.au) | ABN 542 012 184 74



Comcover may wish to consider how they might modify their agency survey of maturity to better assist entities in assessing compliance with the Commonwealth Risk Management Policy.

Yours sincerely



Martin Hehir  
18 July 2017



**Australian Government**

**Department of Health**

**SECRETARY**

18 July 2017

Dr Tom Ioannou  
Group Executive Director  
Performance Audit  
Australian National Audit Office  
GPO Box 707  
Canberra ACT 2601

Dear Dr Ioannou

**Department of Health response to Proposed Report – The Management of Risk by  
Public Sector Entities**

Thank you for providing the Australian National Audit Office's (ANAO) proposed report under s.19 of the *Auditor-General Act 1997* on *The Management of Risk by Public Sector Entities*. I appreciate the opportunity to respond to the report.

The following wording has been provided for the Summary Response:

*I am pleased that the ANAO found that the Department of Health (Health) has met a substantial number of the requirements of the Commonwealth Risk Management Policy. The report demonstrates the progress Health has made to improve its risk management approach and shift to a more risk aware culture. Shifting an organisation's risk culture requires significant commitment from all levels within the organisation and takes time.*

*In April 2017, Health's Accountable Authority endorsed and released a revised Risk Management Policy. This Policy articulates our approach to building a culture of effective risk engagement, where each of us has the skills and confidence to identify and manage risks appropriately.*

*The report has highlighted several areas for improvement in order to strengthen the systems and culture that are required to embed a risk aware culture. Health agrees with these findings and will implement actions to facilitate improvement in these areas.*

---

GPO Box 9848 Canberra ACT 2601

- 2 -

Attachment A to this letter provides detail to the overall response to ANAO's findings relevant to Health.

I would like to thank the ANAO for its professionalism throughout the audit of the Management of Risk by Public Sector Entities.

If you have any questions regarding the Department's response, please contact Mr Ben Sladic on 6289 7735.

Yours Sincerely



Martin Bowles PSM

## AttachmentA

### Areas for Improvement

- *Enhancing risk management capability.*

Agree. Health will continue to move forward with its Risk Management program, including the continued promotion of its risk e-learning modules, to increase risk maturity and focus resources on areas requiring most support.

- *Improving the identification and management of shared risks.*

Agree. Health has enhanced its Health Risk template (which is utilised for business planning) to identify shared risks.

- *Developing arrangements for communicating, consulting and reporting on risk with internal and external stakeholders.*

Agree in principle. Health is currently identifying areas of shared risk with external stakeholders, and within that context will consider the best approach to communicating, consulting and reporting on risk with them.

- *Improving arrangements to regularly review risks, risk management frameworks and the application of risk management practices.*

Agree. Health has commenced implementation with the introduction of risk heat maps for division level and enterprise level risks, and the establishment of a risk maturity map.

- *Seeking formal assurance from managers in preparing responses to the Comcover survey of risk maturity.*

Agree. Health will implement this arrangement during the 2017-18 Comcover survey scheduled for early February 2018.

- *Fully embedding the corporate plan requirement relating to risk.*

Agree. Health's 2017-18 Corporate Plan will include further information on risk.

- *Assigning responsibility for risk management to individuals or positions, rather than work areas.*

Agree. Implementation has commenced. Enterprise level risks are now assigned to Deputy Secretaries with senior governance committees having a stewardship role.



**Australian  
Communications  
and Media Authority**

Level 5  
The Bay Centre  
65 Pirrama Road  
Pyrmont NSW 2009

PO Box C500  
Queen Victoria Building  
NSW 1230

T +61 2 9334 7900  
F +61 2 9334 7711

[www.acma.gov.au](http://www.acma.gov.au)

**Chairman**

19 July 2017

Mr Grant Hehir  
Auditor General  
Australian National Audit Office

[OfficeoftheAuditorGeneralPerformanceAudit@anao.gov.au](mailto:OfficeoftheAuditorGeneralPerformanceAudit@anao.gov.au)

Dear Mr Hehir

#### **The Management of Risk by Public Sector Entities**

Thankyou for the opportunity to participate in the Performance Audit on The Management of Risk by Public Sector Entities. The ACMA has a demonstrated history of effective risk management in the way we conduct our business. The agency values the opportunity to build on our strong foundations through implementing areas for improvement identified by the ANAO.

The findings are timely as the ACMA Risk Management Framework is currently under review and we will keep the ANAO's findings front of mind while making refinements to this framework.

As part of our review, we have already taken steps to address some of the areas for improvement identified by the ANAO. Our Executive Group is releasing a revised Risk Appetite Statement and we are working to ensure our agency has the capability to engage effectively with risk.

The Executive Group has also started the discussion to establish an enduring policy position on the identification and management of shared risk.

We have appointed a Chief Risk Officer to drive improvements to the Risk Management Framework and provide additional support to staff.

I am confident that there is a strong culture of risk management within the ACMA. The insights provided by the ANAO will help us to refine our Risk Management Framework in a way that best supports and builds on that culture.

I would like to express my thanks for the professional and collaborative approach taken by the ANAO audit team during this audit.

Yours sincerely



**Richard Bean**  
Acting Chairman

**communicating | facilitating | regulating**

Page 1 of 1



Australian Government  
Australian Fisheries Management Authority

REF: F2017/0241

Dr Tom Ioannou  
Group Executive Director, Performance Audit  
Australian National Audit Office  
19 National Circuit  
BARTON ACT 2601

Dear Dr Ioannou

Thank you for the opportunity to review and comment on the Australian National Audit Office's (ANAO) Proposed Report on the Management of Risk by Public Sector Entities, provided pursuant to section 19 of the *Auditor-General Act 1997*.

The Australian Fisheries Management Authority (AFMA) acknowledges the supported findings and areas of improvement outlined in this report. AFMA has already begun to act on those findings and we believe the report will help AFMA to further improve our risk management practices in the future.

I would like to express my thanks for the professional and collaborative approach taken by ANAO staff in the conduct of this audit.

Yours sincerely

Dr James Findlay  
Chief Executive Officer

25 July 2017

Canberra  
PO Box 7051  
Canberra Business Centre ACT 2610  
P 02 6225 5555 F 02 6225 5500

Darwin  
PO Box 131  
Darwin NT 0801  
P 08 8943 0333 F 08 8942 2897

Thursday Island  
PO Box 376  
Thursday Island QLD 4875  
P 07 4069 1990 F 07 4069 1277



**Australian Government**  
**Department of Finance**

**Rosemary Huxtable PSM**  
**Secretary**

Our Ref: SEC0014645

Grant Hehir  
Auditor-General  
Australian National Audit Office  
GPO Box 707  
Canberra ACT 2601

Dear Mr Hehir <sup>Grant</sup>

Thank you for the Australian National Audit Office's (ANAO) email of 22 June 2017 regarding the section 19 proposed Audit Report on *The Management of Risk by Public Sector Entities* and seeking the Department of Finance's response.

The Department of Finance thanks the ANAO for the opportunity to respond to the matters raised in the proposed report. Our response is: "The Department of Finance supports the findings of this report".

I welcome the opportunity to work closely with the ANAO to continue to build entities risk capability. The audit's findings will be a useful input for the Department of Finance to target the delivery of Comcover's risk services and the continuing development of the Commonwealth's resource management framework.

Yours sincerely

A handwritten signature in black ink, appearing to read 'RHuxtable', with a long, sweeping horizontal line extending to the right.

Rosemary Huxtable  
Secretary

4 July 2017

## **Appendix 2     The Commonwealth Risk Management Policy requirements**

### **Element 1: Establishing a risk management policy – four requirements**

An entity must establish and maintain an entity specific risk management policy that:

- (a) defines the entity's approach to the management of risk and how this approach supports its strategic plans and objectives;
- (b) defines the entity's risk appetite and risk tolerance;
- (c) contains an outline of key accountabilities and responsibilities for managing and implementing the entity's risk management framework; and
- (d) is endorsed by the entity's accountable authority.

### **Element 2: Establishing a risk management framework – nine requirements**

An entity must establish a risk management framework which includes:

- (a) an overarching risk management policy (Element One);
- (b) an overview of the entity's approach to managing risk;
- (c) how the entity will report risks to both internal and external stakeholders;
- (d) the attributes of the risk management culture that the entity seeks to develop, and the mechanisms employed to encourage this;
- (e) an overview of the entity's approach to embedding risk management into its existing business processes;
- (f) how the entity contributes to managing any shared or cross jurisdictional risks;
- (g) the approach for measuring risk management performance; and
- (h) how the risk management framework and entity risk profile will be periodically reviewed and improved.

The risk management framework must be endorsed by the entity's accountable authority.

### **Element 3: Defining responsibility for managing risk – three requirements**

Within the risk management policy, the accountable authority of an entity must define the responsibility for managing risk by:

- (a) defining who is responsible for determining an entity's appetite and tolerance for risk;
- (b) allocating responsibility for implementing the entity's risk management framework; and
- (c) defining entity roles and responsibilities in managing individual risks.

### **Element 4: Embedding systematic risk management into business processes**

Each entity must ensure that the systematic management of risk is embedded in key business processes.



### **Element 5: Developing a positive risk culture**

An entity's risk management framework must support the development of a positive risk culture.

### **Element 6: Communicating and consulting about risk**

Each entity must implement arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders.

### **Element 7: Understanding and managing shared risk**

Each entity must implement arrangements to understand and contribute to the management of shared risks.

### **Element 8: Maintaining risk management capability**

Each entity must maintain an appropriate level of capability to both implement the entity's risk management framework and manage its risk.

### **Element 9: Reviewing and continuously improving the management of risk**

Each entity must review its risks, its risk management framework and the application of its risk management practices on a regular basis, and implement improvements arising out of such reviews.

Source: The Commonwealth Risk Management Policy, 1 July 2014.

## Appendix 3 ANAO assessment of the selected entities' application of the Commonwealth Risk Management Policy elements

Department of Employment	
Policy elements	ANAO assessment
<b>Element 1: Has Employment established and maintained an entity-specific risk management policy that:</b>	
a) defines the entity's approach to the management of risk and how this approach supports its strategic plans and objectives	<p><b>Met</b></p> <p>Employment's 2016 risk management policy outlines the department's overall approach to risk management. Employment has established a risk management framework that: details the department's approach to the management of risks (risk management policy); provides guidance on managing enterprise and operational risks (<i>Secretary's Instructions</i>); and sets the department's overall risk appetite and risk tolerance (risk appetite and risk tolerance statements).</p> <p>Employment issued its first departmental risk management policy and framework in February 2013. In July 2014—and in response to the release of the Commonwealth Policy—the department released a <i>Secretary's Instruction</i> on its risk management policy and framework. The department updated its 2013 risk management policy and framework in February 2015. This update reflected the department's most recent thinking around risk appetite and tolerance. The department had identified that the application of the risk matrix released in 2013 was resulting in some risks being rated as 'high' that were not significant risks. In September 2016, the risk policy and framework were revised further to include a detailed risk appetite statement.</p>
b) defines the entity's risk appetite and risk tolerance	<p><b>Met</b></p> <p>In September 2016, Employment issued a revised risk appetite and risk tolerance statement that outlined a detailed approach to the department's overall risk appetite and tolerance in the management of risks.</p>
c) contains an outline of key accountabilities and responsibilities for managing and implementing the entity's risk management framework	<p><b>Met</b></p> <p>Employment's risk management policy outlines the assigned key roles and responsibilities for the governance of risk. The <i>Secretary's Instructions (1.1, Risk Management)</i> complement the risk management policy and provide guidance on the department's risk management framework.</p>
d) is endorsed by the entity's accountable authority.	<p><b>Met</b></p> <p>The risk policy and framework were endorsed by the Department's Executive Committee, chaired by the Secretary.</p>

Department of Employment		
Element 2: Has Employment established a risk management framework which includes:		
a) the overarching risk management policy (Element 1)	<b>Met</b> See comments regarding Element 1 (a).	
b) an overview of the entity's approach to managing risk	<b>Met</b> Employment's risk management framework refers to the <i>Secretary's Instruction</i> on risk management which outlines the department's approach to the management of risks, including the key roles and responsibilities in managing risks by: the Executive; governance committees; the Risk, Assurance and Performance Section (RAPS); and all departmental officials.	
c) how the entity will report risks to both internal and external stakeholders	<b>Mostly met</b> Employment's risk management framework was developed with extensive internal consultation, including with the audit committee. The framework does not explicitly outline arrangements for communicating, consulting and reporting about risk with internal and external stakeholders. Employment advised the ANAO that in practice consultation on risk occurs as part of its routine consultation and interaction with external stakeholders and other Commonwealth entities.	
d) the attributes of the risk management culture that the entity seeks to develop, and the mechanisms employed to encourage this	<b>Met</b> The framework outlines the attributes of the department's risk management culture. The framework also outlines the way the department intends to measure its risk culture through: staff census results; internal and external audits; measures of compliance; regular reviews and monitoring of risk practices throughout the department; and engagement with training offered.	
e) an overview of the entity's approach to embedding risk management into its existing business processes	<b>Met</b> The framework outlines how the department proposes to embed risk management into its existing business processes, including: assurance mechanisms; and processes relating to the direction, oversight and approval of risks.	
f) how the entity contributes to managing any shared or cross jurisdictional risks	<b>Met</b> The 2016 risk management framework refers to the department's approach to recognising and managing shared risks, specifically mentioning the Shared Services Centre, other government agencies and third-party employment providers.	
g) the approach for measuring risk management performance	<b>Met</b> The framework indicates that the performance of the department's risk management framework is assessed against the achievement of four risk management objectives: organisational resilience; positive risk culture; integrated and consistent application; and informed and effective decision making.	

Department of Employment	
h) how the risk management framework and entity risk profile will be periodically reviewed and improved.	<b>Met</b> The framework outlines how the framework will be reviewed.
i) The risk management framework is endorsed by the entity's accountable authority.	<b>Met</b> See comments regarding Element 1 (d).
<b>Element 3: Has the accountable authority of Employment defined the responsibility for managing risk, by:</b>	
a) defining who is responsible for determining the entity's appetite and tolerance for risk	<b>Met</b> The department's risk appetite and tolerance statement was approved by the Executive Committee and issued by the Secretary in line with the <i>Secretary's Instructions</i> .
b) allocating responsibility for implementing the entity's risk management framework	<b>Met</b> The Risk, Assurance and Performance Section (RAPS) within the Assurance and Business Services Branch is responsible for implementing the department's enterprise risk management framework, and ensuring the framework and risk profile remain current and relevant.
c) defining entity roles and responsibilities in managing individual risks.	<b>Met</b> The risk management policy outlines responsibilities for risk management, with further detail contained in the <i>Secretary's Instructions</i> .

Department of Employment	
<b>Element 4: Has Employment ensured that the systematic management of risk is embedded in key business processes?</b>	
	<p><b>Met</b></p> <p>Employment's Risk and Implementation Committee (ERIC) met six times each year in 2014, 2015 and 2016 to consider and oversight the operations of the department's risk management policy and framework, and reported regularly to the department's executive committee on the adequacy of the risk framework and associated processes.</p> <p>ERIC was disbanded in December 2016. Employment records indicate that its risk responsibilities were divided between the Audit Committee—responsible for risk assurance—and the Finance and Business Services (FABS) Committee—responsible for risk framework implementation, monitoring and improvement (see Element 9 below).</p> <p>The department's Performance and Integrity Sub Committee for Employment Services (PISCES) provides a high-level forum to support and advise on maximising the performance and integrity of all contracted employment services under jobactive. The department's Audit Committee also regularly receives updates from management on aspects of the department's risk framework and obtains presentations from time to time from responsible departmental managers on the management of risks in respect of specific programs or activities. The operational divisions reviewed by the ANAO employed the department's enterprise-wide risk management system (RiskActive) to assist in managing risk.</p>
<b>Element 5: Does Employment's risk management framework support the development of a positive risk culture?</b>	
	<p><b>Met</b></p> <p>To assess the selected entities' implementation of the overarching goal of the Commonwealth Policy and its policy element five—developing a positive risk culture—the ANAO had regard to: entities' implementation of the Commonwealth Policy requirements; risk management in a selection of business activities in each entity; and the consideration of risk by senior leaders.</p> <p>Employment met 19 and mostly met two of the requirements (total 21/22 or 95 per cent).</p> <p>The ANAO's review of a selection of business activities (see footnote 37) indicates that risk management informs normal business operations in the selected entities. Risk was considered when key business decisions were made or advice was provided to senior management or government by the areas selected for review.</p> <p>The risk management framework and key risks were regularly considered at senior levels (see comments regarding Element 4 above).</p>

Department of Employment	
<b>Element 6: Has Employment implemented arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders?</b>	
	<p><b>Mostly met</b></p> <p>The department has: extensive risk management guidance available on its Intranet; provides assistance on risk management to staff through an internal hotline; and management reporting arrangements that reinforce the importance of risk management.</p> <p>The development of the new Risk Appetite and Tolerance Statement and the supporting methodology involved extensive internal consultation.</p> <p>It is not evident that the development of the above artefacts involved consultation with external stakeholders.</p> <p>Employment advised the ANAO that in practice consultation on risk occurs as part of the department's routine consultation and interaction with external stakeholders and other Commonwealth entities.</p>
<b>Element 7: Has Employment implemented arrangements to understand and contribute to the management of shared risks?</b>	
	<p><b>Partly met</b></p> <p>Departmental records indicate that shared risks were identified and managed in relation to the Shared Services Centre, prior to its transfer to the Department of Finance.</p> <p>Employment did not routinely categorise and manage shared risks other than risks relating to the Shared Services Centre. It is not evident that other risks are recognised in departmental risk registers and managed as shared risks, and risk reporting does not include reporting on shared risks. See also comments regarding Element 2 (f).</p>
<b>Element 8: Has Employment maintained an appropriate level of capability to both implement the entity's risk management framework and manage its risks?</b>	
	<p><b>Met</b></p> <p>The department has extensive guidance and tools available to staff to assist with the management of risk. Training courses, including eLearning modules are available to all staff. The department has a dedicated Risk, Assurance and Performance Section within the Assurance and Business Services Branch that provides support to operational areas on managing their risks.</p> <p>The department operates and maintains an enterprise-wide risk management systems to assist in managing its risks—<i>RiskActive</i>. The system is mature and provides the department with the capability to record, manage and report on risks, risk treatments, risk events and risk plan owners.</p>

Department of Employment	
Element 9: Does Employment review its risks, its risk management framework and the application of its risk management practices on a regular basis, and implement improvements arising out of such reviews?	
	<p><b>Met</b></p> <p>The framework has been updated at least annually—in July 2014, February 2015, and September 2016. Employment's Risk and Implementation Committee (ERIC) reviewed the department's strategic risks at least quarterly and risk plan owners were required to review risks on a regular basis. ERIC received regular reports on the department's risk profile and on whether risk plan owners and treatment owners were meeting their responsibilities.</p> <p>Following a 2016 review of governance committees, ERIC was disbanded in December 2016 and the Finance and Business Services Committee (FABS) was given responsibility to advise the Secretary on: risks identified in relation to the department's ability to meet its business goals, as per the Risk Management Framework; and work to improve the department's risk and policy framework, and lead the application of risk management across the department. At its meeting in March 2017, the FABS noted that the department's Executive had participated in a workshop to review entity strategic risks in February 2017; and considered an entity-level risk monitoring report. The FABS terms of reference require it to report to the Executive on a quarterly basis and state that the co-chairs will provide an oral update to the Executive as needed.</p>

Department of Health	
Policy elements	ANAO assessment
<b>Element 1: Has Health established and maintained an entity-specific risk management policy that:</b>	
a) defines the entity's approach to the management of risk and how this approach supports its strategic plans and objectives	<p><b>Met</b></p> <p>Health's 2014 risk management policy outlines the department's overall approach to risk management. Health issued a revised departmental risk management policy and framework in October 2014, three months after the release of the Commonwealth Policy. The department's 2014 risk management policy states that the policy should be reviewed and updated annually. In December 2016, Health released a new risk appetite following extensive internal consultation.</p>
b) defines the entity's risk appetite and risk tolerance	<p><b>Met</b></p> <p>In December 2016, Health issued an updated enterprise risk appetite statement that detailed approach to the department's overall risk appetite and tolerance in the management of risks.</p>
c) contains an outline of key accountabilities and responsibilities for managing and implementing the entity's risk management framework	<p><b>Met</b></p> <p>Health's risk management policy outlines the assigned key roles and responsibilities for the governance of risk.</p>
d) is endorsed by the entity's accountable authority.	<p><b>Mostly met</b></p> <p>The risk management policy and framework were endorsed by the Finance, Risk and Security Committee, which is chaired by a Deputy Secretary. The Committee is a sub-committee of the department's executive committee, chaired by the Secretary. It was not evident that the 2014 policy was endorsed by the Secretary; however, the December 2016 risk appetite statement was endorsed by the Secretary.</p>
<b>Element 2: Has Health established a risk management framework which includes:</b>	
a) the overarching risk management policy (Element 1)	<p><b>Met</b></p> <p>See comments regarding Element 1 (a).</p>
b) an overview of the entity's approach to managing risk	<p><b>Met</b></p> <p>Health encourages staff to engage with, understand and appropriately manage its risks. Specifically, the department seeks to engage with higher levels of risk and look for innovation, in relation to its policy development and delivery outcomes where the potential rewards may provide improvements to the health and well-being of the Australian public.</p>



Department of Health	
c) how the entity will report risks to both internal and external stakeholders	<p><b>Mostly met</b></p> <p>Health's risk management framework was developed with extensive internal consultation, including with the audit committee. The framework does not explicitly outline arrangements for communicating, consulting and reporting about risk with internal and external stakeholders. Health advised the ANAO that in practice consultation on risk occurs as part of its routine consultation and interaction with external stakeholders and other Commonwealth entities.</p>
d) the attributes of the risk management culture that the entity seeks to develop, and the mechanisms employed to encourage this	<p><b>Met</b></p> <p>The policy lists leadership, communication, integration and responsibility as being the key drivers of a positive risk culture.</p>
e) an overview of the entity's approach to embedding risk management into its existing business processes	<p><b>Mostly met</b></p> <p>The policy states that 'Risk management is an essential element of sound business planning, change management and decision making in the department'. The policy could be more explicit about how this will be achieved.</p>
f) how the entity contributes to managing any shared or cross jurisdictional risks	<p><b>Mostly met</b></p> <p>Health's risk management policy discusses the importance of identifying and managing shared risks. The department's risk register template includes a field for the identification of shared risks and a number of Divisional risk registers included a number of shared risks.</p> <p>There was some confusion about the definition of shared risk. Some of the risks identified as shared risks were risks that were shared with other areas of the department. There is no guidance on managing shared risks and no formal reporting of shared risks. The department was not able to demonstrate how shared risks have been managed, once they were identified in Risk Management Plans.</p>
g) the approach for measuring risk management performance	<p><b>Met</b></p> <p>The policy states that performance will be measured by the annual Comcover benchmarking survey. Consideration could also be given to other mechanisms for measuring risk management performance, such as the development of key performance indicators and the conduct of surveys that address risk culture.</p>
h) how the risk management framework and entity risk profile will be periodically reviewed and improved.	<p><b>Met</b></p> <p>The framework outlines how the framework will be reviewed.</p>
i) The risk management framework is endorsed by the entity's accountable authority.	<p><b>Mostly met</b></p> <p>See comments regarding Element 1 (d).</p>

Department of Health	
<b>Element 3: Has the accountable authority of Health defined the responsibility for managing risk, by:</b>	
a) defining who is responsible for determining the entity's appetite and tolerance for risk	<p><b>Met</b> The policy states that Health's management and governance committees are required to articulate the risk appetite for increasing risk and risk boundaries.</p>
b) allocating responsibility for implementing the entity's risk management framework	<p><b>Mostly met</b> The Risk Management Policy states that the Office of the Chief Financial Officer is responsible for managing and implementing Health's Risk Management Policy and Framework. However the <i>Finance Business Rules</i> state that the Integrity Branch is responsible for this role.</p>
c) defining entity roles and responsibilities in managing individual risks.	<p><b>Met</b> The risk management policy outlines responsibilities for risk management.</p>
<b>Element 4: Has Health ensured that the systematic management of risk is embedded in key business processes?</b>	
	<p><b>Mostly met</b> Key risks were regularly considered by Health's executive committee in its consideration of specific departmental strategies and plans, and the three operational divisions examined by the ANAO had established a range of local mechanisms to monitor, report on and manage risk. Health's 2015 review of risk management practices observed that the management of risk across the department was more likely to be dealt with appropriately where there was a strong legislative requirement, as in the regulatory work of the Office of the Gene Technology Regulator, and less so in the operational areas.</p>

Department of Health	
Element 5: Does Health's risk management framework support the development of a positive risk culture?	
	<p><b>Mostly met</b></p> <p>To assess the selected entities' implementation of the overarching goal of the Commonwealth Policy and its policy element five—developing a positive risk culture—the ANAO had regard to: entities' implementation of the Commonwealth Policy requirements; risk management in a selection of business activities in each entity; and the consideration of risk by senior leaders.</p> <p>Health met 10 and mostly met 10 of the requirements (total 20/22 or 91 per cent).</p> <p>The ANAO's review of a selection of business activities (see footnote 37) indicates that risk management informs normal business operations in the selected entities. Risk was considered when key business decisions were made or advice was provided to senior management or government by the areas selected for review.</p> <p>Key risks were regularly considered by Health's executive committee in its consideration of specific departmental strategies and plans. There is scope for a more structured approach to reporting on and reviewing enterprise-level risks and the status of risk controls and treatments. The three operational divisions examined by the ANAO had established a range of local mechanisms to monitor, report on and manage risk.</p>
Element 6: Has Health implemented arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders?	
	<p><b>Mostly met</b></p> <p>The Health Capability Program was initiated in early 2015 to address the findings of the 2014 Health Capability Review, including the need to foster a culture that appropriately embraces and manages risks within defined tolerances. The capability program conducted extensive internal consultations, including engagement with over 1000 staff through the Senior Management Forum (SES forum), a series of executive leadership forums (EL Forums) and over 30 focus groups.</p> <p>Health has recently introduced a new stakeholder management system <i>Engage</i> for the identification and reporting of risks. Arrangements for reporting on risk to external stakeholders are unclear.</p> <p>Health advised the ANAO that in practice consultation on risk occurs as part of the routine consultation and interaction with external stakeholders and other Commonwealth entities.</p>

Department of Health	
Element 7: Has Health implemented arrangements to understand and contribute to the management of shared risks?	
	<p><b>Partly met</b></p> <p>Health's risk management policy defines shared risks and the department's risk register templates make provision for recording them. The ANAO's review identified that some of the assigned shared risks were intra-entity—such as risks shared with other areas of the department—whereas the Commonwealth Policy defines a shared risk as one extending beyond the entity. See also comments regarding Element 2(f).</p>
Element 8: Has Health maintained an appropriate level of capability to both implement the entity's risk management framework and manage its risks?	
	<p><b>Mostly met</b></p> <p>Health's risk-related intranet page contains guidance, FAQ sheets and contact details for the corporate risk team. As part of the progressive enhancement of the department's risk management framework, a Risk Tool Kit is being developed but had not been finalised at the time of the audit.</p> <p>All staff can access a risk management e-learning module, or attend two health-specific face-to-face training sessions, which are encouraged through individual performance development plans. The e-learning module was introduced in January 2017, but there has been limited uptake of these training sessions, and as at April 2017 approximately 0.01 per cent of Health employees had attended specific risk management training.</p> <p>Health staff can access Risk Management training in other courses, for example the APSC Procurement and Contracts Management Training. Health also encourages SES to attend the Comcover Risk Workshops, and has also held a variety of workshops for SES and EL2 staff on risk, controls and shared risk in 2016 and 2017.</p> <p>A risk register template is available to divisions and 20 of the 21 divisions have established a risk register. At the time of the audit this template had not been updated to reflect the risk categories outlined in the new Risk Appetite statement. Until late in 2016 there was little or no corporate review or oversight of divisional risk registers and there were no arrangements in place for the department's Executive to be assured that risk registers are complete and up-to-date.</p> <p>The department has staff resources dedicated to risk management of 3.2 ASL in its Risk and Business Assurance Section. There is also a dedicated risk management mailbox.</p>

Department of Health	Element 9: Does Health review its risks, its risk management framework and the application of its risk management practices on a regular basis, and implement improvements arising out of such reviews?	
		<p><b>Partly met</b></p> <p>The current risk management policy was approved in October 2014. An updated risk appetite statement was released in December 2016. A revised risk management policy had been drafted at the time of this audit but had yet to be approved and issued. There is no consolidated reporting to the department's executive on the state of the department's risk profile and risks.</p> <p>The Risk and Business Assurance section commenced a review of all divisional risk registers as a quality assurance project in late 2016. Prior to this initiative, the section had very little visibility of divisional risk registers and risk management practices. Health advised the ANAO in April 2017 that the review was completed in February 2017. Health provided an update to the ANAO in June 2017 that the Executive Committee was provided with a report on risk maturity across the department, and assigned responsibility for the strategic risks to individuals.</p> <p>All divisions are required to create and update risk registers, to identify and assess risks and assign responsibilities for managing risks. Most divisions have established these registers, but it was not evident that the registers were reviewed quarterly, as required by Health's Risk Management Policy, or that the registers were used to actively manage risks within each division. Four divisions had not established a risk register at the time of this audit.</p> <p>In June 2016 the Executive Committee was advised that it was intended that each division develop a risk register, and that all registers would be collated into an Enterprise Risk Profile and reported to the Executive Committee. At the time of this audit this reporting had not commenced.</p> <p>At the time of the audit, there was limited management reporting to the executive committee on the status of enterprise-level risks, as part of a structured process of regular review of enterprise-level risks, controls and treatments.</p> <p>The department does not systematically record and analyse incidents and risk events to inform any review of risk practices and the risk framework. Staff responsible for managing grants are required to maintain a record of risk events and to escalate high risks immediately.</p> <p>One of the aims of the Health Capability Program is to develop a common understanding and approach to recognising and managing risk. At the time of this audit, the risk-related aspect of the Program remained a work in progress.</p>

Australian Communications and Media Authority (ACMA)		
Policy elements	ANAO assessment	
Element 1: Has ACMA established and maintained an entity-specific risk management policy that:		
a) defines the entity's approach to the management of risk and how this approach supports its strategic plans and objectives	<b>Mostly met</b> ACMA issued a revised risk management guide and management instruction in July 2015, 12 months after the release of the Commonwealth Policy.  ACMA's risk management guide outlines the Authority's overall approach to risk management, but is limited to definitions of concepts and generic statements in accordance with AS/NZS ISO 31000:2009 Risk Management Principles. It provides a high-level description of risk management but limited practical guidance on how staff should manage risk.	
b) defines the entity's risk appetite and risk tolerance	<b>Partly met</b> In July 2015, ACMA issued a risk tolerance statement but did not define its risk appetite statement.  ACMA's risk tolerance is described as being 'as low as reasonably practicable' (ALARP). ACMA was not able to demonstrate to the ANAO how the ALARP approach was used in practice. Further, ACMA does not provide any guidance on assessing the cost-benefits of risk mitigation activities, a requirement of the ALARP approach.	
c) contains an outline of key accountabilities and responsibilities for managing and implementing the entity's risk management framework	<b>Met</b> ACMA's risk management guide outlines the assigned key roles and responsibilities for the governance of risk.	
d) is endorsed by the entity's accountable authority.	<b>Mostly met</b> The Chair of ACMA endorsed the risk management instruction, and the Governance and Security Manager authorised the risk management guide.	
Element 2: Has ACMA established a risk management framework which includes:		
a) the overarching risk management policy (Element 1)	<b>Mostly Met</b> See comments regarding Element 1 (a).	
b) an overview of the entity's approach to managing risk	<b>Met</b> ACMA's risk management guide outlines the Authority's overall approach to risk management.  ACMA's risk management guide and instruction also refer to the responsibilities of the Accountable Authority, the Audit and Risk Committee and the Governance and Security Manager for managing risks.	

Australian Communications and Media Authority (ACMA)	
c) how the entity will report risks to both internal and external stakeholders	<p><b>Partly met</b></p> <p>ACMA's risk management framework was developed with extensive internal consultation, including with the audit committee. The framework does not explicitly outline arrangements for communicating, consulting and reporting about risk with internal stakeholders. The internal reporting of risks is discussed in broad terms in the Guide. The Guide does not outline how ACMA intends to consult or report on risks to either internal or external stakeholders.</p>
d) the attributes of the risk management culture that the entity seeks to develop, and the mechanisms employed to encourage this	<p><b>Partly met</b></p> <p>ACMA's risk management guide states that "the Agency strives to have a robustly structured risk management culture", and if a person's work seamlessly considers risk, or risk management is integrated into day-to-day activities, then a healthy risk management culture exists.</p> <p>ACMA could outline in more detail the attributes of the risk management culture that it seeks to develop.</p>
e) an overview of the entity's approach to embedding risk management into its existing business processes	<p><b>Met</b></p> <p>ACMA's risk management guide sets out a risk management framework and risk management processes, including a set of instructions to assist staff to identify, document and assess risk within the stated tolerance levels. ACMA's risk management guidance provides a high-level description of risk management, but limited practical guidance on how staff should manage risk. That said, templates are provided to the divisions and support is provided when required to assist with the risk management process.</p>
f) how the entity contributes to managing any shared or cross jurisdictional risks	<p><b>Not met</b></p> <p>ACMA does not refer to shared risk in its risk guidance and instruction, and there is no explanation of how shared risks should be identified and managed.</p>
g) the approach for measuring risk management performance	<p><b>Partly met</b></p> <p>The performance section of the guide is generic in nature, and as such does not specifically relate to measuring performance of risk at ACMA.</p> <p>The guide states that: risk treatment plans should include performance measures; mitigation measures should be measured for effectiveness; and higher level organisational performance indicators and measures should be used to judge the performance of risk management.</p>
h) how the risk management framework and entity risk profile will be periodically reviewed and improved.	<p><b>Mostly met</b></p> <p>ACMA's 2015 risk management guidance states that the policy should be reviewed and updated annually. The guide was due to be reviewed in the second half of 2016. ACMA advised the ANAO that it has decided to await the outcomes of this audit before finalising its review.</p>

Australian Communications and Media Authority (ACMA)	
i) The risk management framework is endorsed by the entity's accountable authority.	<p><b>Mostly met</b></p> <p>See comments regarding Element 1 (d).</p>
<b>Element 3: Has the accountable authority of ACMA defined the responsibility for managing risk, by:</b>	
a) defining who is responsible for determining the entity's appetite and tolerance for risk	<p><b>Mostly met</b></p> <p>There is a broad statement in ACMA's risk management guide of the Accountable Authority's responsibilities, but the statement does not explicitly define who is responsible for determining the risk appetite and tolerance.</p>
b) allocating responsibility for implementing the entity's risk management framework	<p><b>Met</b></p> <p>ACMA's Governance and Security Manager is responsible for the day-to-day maintenance and promotion of ACMA's risk management framework. ACMA have recently engaged a Risk Manager.</p>
c) defining entity roles and responsibilities in managing individual risks	<p><b>Met</b></p> <p>The Guide outlines responsibilities for strategic, Divisional and program/project risks. The Guide also states that risks need to be allocated to a risk owner, to ensure there is accountability for, and ownership of, the risks.</p>
<b>Element 4: Has ACMA ensured that the systematic management of risk is embedded in key business processes?</b>	
	<p><b>Met</b></p> <p>ACMA's key risks were reviewed quarterly by the senior executive as part of a regular cycle. Staff were able to show that an assessment of risk informed local decision making processes, and that risk conversations at the senior and middle management levels took place. At an operational level, delegations for decision making relating to broadcasting and datacasting investigations are based on the assessed level of risk of each investigation.</p>



Australian Communications and Media Authority (ACMA)	
Element 5: Does ACMA's risk management framework support the development of a positive risk culture?	
	<p><b>Mostly met</b></p> <p>To assess the selected entities' implementation of the overarching goal of the Commonwealth Policy and its policy element five—developing a positive risk culture—the ANAO had regard to: entities' implementation of the Commonwealth Policy requirements; risk management in a selection of business activities in each entity; and the consideration of risk by senior leaders.</p> <p>ACMA met six and mostly met 10 of the requirements (total 16/22 or 73 per cent).</p> <p>The ANAO's review of a selection of business activities (see footnote 37) indicates that risk management informs normal business operations in the selected entities. Risk was considered when key business decisions were made or advice was provided to senior management or government by the areas selected for review.</p> <p>The risk management framework and key risks were regularly considered at senior levels (see comments regarding Element 4 above).</p>
Element 6: Has ACMA implemented arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders?	
	<p><b>Mostly met</b></p> <p>ACMA has: risk management guidance available on its Intranet; provides assistance on risk management through a dedicated Risk Officer; and management reporting arrangements that reinforce the importance of risk management.</p> <p>ACMA's Audit and Risk Committee receives quarterly updates on the risk management framework, including new and emerging risks.</p> <p>ACMA did not communicate or consult with its external stakeholders in the development of its risk framework but the ANAO was advised that risk is routinely discussed with external stakeholders and other entities in the conduct of its regulatory activities. ACMA was able to provide examples where projects and issues were discussed between ACMA and Defence, and between ACMA and the Department of Finance.</p>
Element 7: Has ACMA implemented arrangements to understand and contribute to the management of shared risks?	
	<p><b>Partly met</b></p> <p>ACMA does not refer to shared risk in its risk guidance and instruction, and there is no explanation of how shared risks should be identified and managed. In practice, ACMA and its portfolio department have created a shared risk register for their joint steering committee. ACMA advised the ANAO that arrangements for identifying and managing shared risks will be developed as part of a planned review of the risk framework.</p>

Australian Communications and Media Authority (ACMA)	
<b>Element 8: Has ACMA maintained an appropriate level of capability to both implement the entity's risk management framework and manage its risks?</b>	
	<p><b>Mostly met</b></p> <p>ACMA has developed risk templates and guidance to assist staff in the management of risks. ACMA also has a variety of training material available to staff. As at 14 December 2016, 79 per cent of ACMA employees had completed the compulsory risk management e-learning module. ACMA has recently hired a Risk Officer, and filled the position of Manager, Governance and Security which has responsibility for risk at a corporate level.</p>
<b>Element 9: Does ACMA review its risks, its risk management framework and the application of its risk management practices on a regular basis, and implement improvements arising out of such reviews?</b>	
	<p><b>Mostly met</b></p> <p>ACMA's risk registers are reviewed and updated every quarter. Division managers provide a written confirmation to the Executive Group confirming that the registers have been reviewed, and that the controls are adequate and operational. In addition, the risk officer reviews the active controls in the risk registers and advises each division how to make improvements.</p> <p>The more timely review and updating of ACMA's risk management framework would provide consistent corporate messaging on ACMA's appetite for, and management of, risk. There is also scope for risk events and incidents to be recorded and analysed. This could be considered as part of the review of risk management practices.</p> <p>ACMA's Guide and Instruction were due to be reviewed in July 2016, but this had not occurred at the time of the audit. See comments regarding Element 2(h).</p>

Australian Fisheries Management Authority (AFMA)		
Policy elements	ANAO assessment	
Element 1: Has AFMA established and maintained an entity-specific risk management policy that:		
a) defines the entity's approach to the management of risk and how this approach supports its strategic plans and objectives	<b>Met</b> AFMA's 2016 risk management policy outlines the Authority's overall approach to risk management. AFMA issued a revised risk management framework in February 2015 seven months after the release of the Commonwealth Policy. The authority released an updated risk management policy, which included a risk appetite statement, in November 2016. AFMA issued risk management operational guidelines in February 2017.	
b) defines the entity's risk appetite and risk tolerance	<b>Met</b> In November 2016, AFMA issued an enterprise risk appetite and tolerance statement that detailed the Authority's overall risk appetite and tolerance in the management of risks in a number of key risk areas.	
c) contains an outline of key accountabilities and responsibilities for managing and implementing the entity's risk management framework	<b>Met</b> AFMA's risk management policy outlines the assigned key roles and responsibilities for the governance of risk. The policy incorporates a table that links corporate goals to risk areas and the Authority's risk management response.	
d) is endorsed by the entity's accountable authority.	<b>Met</b> The November 2016 risk management policy and February 2107 risk management guidelines were endorsed by the Chief Executive.	
Element 2: Has AFMA established a risk management framework which includes:		
a) the overarching risk management policy (Element 1)	<b>Met</b> See comments regarding Element 1 (a).	
b) an overview of the entity's approach to managing risk	<b>Met</b> The risk management framework refers to the risk management policy and guidelines which outline the Authority's approach to the management of risk, including key roles and responsibilities in managing risks, internal (but not external) consultation arrangements, and arrangements for monitoring the performance of staff in risk management activities.	

Australian Fisheries Management Authority (AFMA)	
c) how the entity will report risks to both internal and external stakeholders	<p><b>Partly met</b></p> <p>AFMA's risk management guidelines address internal and external consultation arrangements, as an input to an organisational risk register that supports the internal reporting of risks to the CEO, Commission and the Audit and Risk Committee. These arrangements had not been implemented at the time of this audit, and an enterprise-level risk register had yet to be created.</p> <p>The guidelines do not refer to arrangements for reporting risks to external stakeholders.</p>
d) the attributes of the risk management culture that the entity seeks to develop, and the mechanisms employed to encourage this	<p><b>Partly met</b></p> <p>The policy and guidelines do not specifically outline the attributes of a risk management culture that the Authority seeks to develop. The risk management policy outlines arrangements for staff-directed assessments to be undertaken and for reviews of risks and treatments outlined in position descriptions to be undertaken every 12 months. The framework and policy do not otherwise describe the mechanisms for encouraging the achievement of a risk management culture.</p>
e) an overview of the entity's approach to embedding risk management into its existing business processes	<p><b>Met</b></p> <p>The guidelines outline the procedures for identifying, analysing and treating risk; set out the Authority's expectations that all staff have an awareness of, and be engaged with, managing risks, including training, staff-directed assessments, and reporting arrangements and responsibilities.</p>
f) how the entity contributes to managing any shared or cross jurisdictional risks	<p><b>Met</b></p> <p>AFMA's February 2017 risk management guidelines addressed the issue of establishing shared risks through external consultation processes:</p> <p>External consultation will establish shared risks through engagement with other Commonwealth agencies, cross-jurisdictional entities, industry and interest groups. Once every 12 months AFMA's Risk Manager will engage with external stakeholders to establish the register of shared risks and report the findings to the Audit and Risk Committee and the AFMA Commission.</p>
g) the approach for measuring risk management performance	<p><b>Partly met</b></p> <p>The policy and guidelines indicate that managers and senior managers should monitor the performance of staff in risk management activities, including the maintenance of controls, implementation of new treatments and the identification of new risks. There is, however, no explicit approach outlined for measuring risk management performance.</p> <p>AFMA advised that it has relied on Comcover's annual benchmarking survey and renewal questionnaire on risk management processes to assess risk management performance.</p>

Australian Fisheries Management Authority (AFMA)	
h) how the risk management framework and entity risk profile will be periodically reviewed and improved.	<p><b>Met</b></p> <p>AFMA's November 2016 risk management policy states that the Risk Manager is responsible for the ongoing maintenance of risk registers and reporting to the CEO, AFMA Commission, Risk Management Committee and the Audit and Risk Committee. The policy and guidelines task the Risk Management Committee with responsibility for reviewing AFMA's risk management framework once each year, including the risk register and risk management plans. These arrangements were not fully implemented at the time of this audit.</p>
i) The risk management framework is endorsed by the entity's accountable authority.	<p><b>Met</b></p> <p>See comments regarding Element 1 (d).</p>
<b>Element 3: Has the accountable authority of AFMA defined the responsibility for managing risk, by:</b>	
a) defining who is responsible for determining the entity's appetite and tolerance for risk	<p><b>Met</b></p> <p>AFMA's November 2016 risk management policy states that the Chief Executive is responsible for approving the Authority's risk appetite and tolerance as part of approving the Risk Management Policy.</p>
b) allocating responsibility for implementing the entity's risk management framework	<p><b>Met</b></p> <p>The CEO has established a risk management committee with specified responsibilities. The risk management committee is intended to provide an intra-entity perspective, review the risk management framework once each year and monitor adherence of staff to the guidelines. The risk manager is responsible for maintenance of the organisational risk register and coordination of reporting to the Executive and audit and risk committee.</p>
c) defining entity roles and responsibilities in managing individual risks.	<p><b>Met</b></p> <p>AFMA guidance outlines roles and responsibilities for managing risks. There is scope to review AFMA's consolidated risk register, which is used to collate risks from across the entity, as the majority of risks in the register were assigned to a work area rather than an individual or position and in some cases certain risks were not assigned.</p>

Australian Fisheries Management Authority (AFMA)	
Element 4: Has AFMA ensured that the systematic management of risk is embedded in key business processes?	
	<p><b>Mostly met</b></p> <p>Sustainability risks were regularly considered by the AFMA Commission in its consideration of specific fisheries management strategies and plans. Available records indicated that the operational branch selected for review had produced a range of risk assessments and guidance on risk management. There is scope for a more structured approach to reporting on and reviewing enterprise-level risks, controls and treatments.</p>
Element 5: Does AFMA's risk management framework support the development of a positive risk culture?	
	<p><b>Partly met</b></p> <p>To assess the selected entities' implementation of the overarching goal of the Commonwealth Policy and its policy element five—developing a positive risk culture—the ANAO had regard to: entities' implementation of the Commonwealth Policy requirements; risk management in a selection of business activities in each entity; and the consideration of risk by senior leaders.</p> <p>AFMA met 13 and mostly met two of the requirements (total 15/22 or 68 per cent).</p> <p>The ANAO's review of a selection of business activities (see footnote 37) indicates that risk management informs normal business operations in the selected entities. Risk was considered when key business decisions were made or advice was provided to senior management or government by the areas selected for review. For example, the Fisheries Management Branch had risk management practices embedded as part of its core decision making processes under the Ecological Risk Management Framework.</p> <p>The risk management framework and key risks were regularly considered at senior levels (see comments regarding Element 4 above).</p>

## Australian Fisheries Management Authority (AFMA)

**Element 6: Has AFMA implemented arrangements to communicate and consult about risk in a timely and effective manner to both internal and external stakeholders?**

### Mostly met

The development of the risk policy and guidelines involved consultation with senior management, the Audit Committee and the Commission, which comprises six external members. The development of the policy, including the risk appetite and tolerance, did not involve consultation with other external stakeholders.

The consultation arrangements outlined in the policy and guidelines had not been fully implemented at the time of the audit.

The Fisheries Management Branch risk assessment processes include communicating and consulting with resource assessment groups, technical support groups and management advisory committees. These groups and committees are comprised of representatives from the scientific community and stakeholder groups.

**Element 7: Has AFMA implemented arrangements to understand and contribute to the management of shared risks?**

### Partly met

AFMA is in the early stages of implementing its risk guidelines and its approach to external consultation and shared risks. AFMA's February 2017 risk management guidelines addressed the issue of establishing shared risks through external consultation processes:

External consultation will establish shared risks through engagement with other Commonwealth agencies, cross-jurisdictional entities, industry and interest groups. Once every 12 months AFMA's Risk Manager will engage with external stakeholders to establish the register of shared risks and report the findings to the Audit and Risk Committee and the AFMA Commission.

These arrangements were not implemented and no shared risks had been identified at the time of this audit.

Australian Fisheries Management Authority (AFMA)	
Element 8: Has AFMA maintained an appropriate level of capability to both implement the entity's risk management framework and manage its risks?	<p><b>Partly met</b></p> <p>Risk management guidance available on AFMA's Intranet was minimal and not up to date. Other risk-related guidance available on the Intranet focussed on project management, and did not include guidance for business as usual activities. Project management templates, including a register, were available to identify, monitor and report on project risks.</p> <p>AFMA does not have formal learning and development programs in risk management for staff. The ANAO was advised by AFMA that work had commenced to implement a training package for staff on the <i>Public Governance, Performance and Accountability (PGPA) Act 2013</i>, including a risk management module.</p>
Element 9: Does AFMA review its risks, its risk management framework and the application of its risk management practices on a regular basis, and implement improvements arising out of such reviews?	<p><b>Partly met</b></p> <p>AFMA conducted a review of its risk management framework in June 2015 but was slow in addressing the findings and recommendations of the review. The consolidated risk register became non-operational, resulting in a lack of recording, reporting and review of risks at a corporate and strategic level. The risk management committee responsible for oversight and review of the framework did not meet for over two years and reconvened for the first time in December 2016.</p> <p>With regard to the Fisheries Management Branch, the Ecological Risk Management Guide was being revised during 2016 in response to a review that was conducted between 2012 and 2014. AFMA advised the ANAO in June 2017 that the revised Guide was approved by the Commission in March 2017.</p> <p>At the time of the audit, there was limited management reporting to the Commission on the status of enterprise-level risks, as part of a structured process of regular review of enterprise-level risks, controls and treatments.</p>



## Appendix 4 Health's Enterprise Risk Appetite statement

### Department of Health ENTERPRISE RISK APPETITE



Australian Government  
Department of Health



#### Risk appetite

The risk appetite for the department outlines where we are willing to engage with higher levels of risk for a greater benefit and to achieve our strategic objectives. Understanding our risk appetite assists in decision making across the department but may vary between business areas, depending on the work being carried out.

#### Our risk appetite statement

The department wants everyone to engage with, understand and appropriately manage its risks. Specifically, the department is eager to engage with higher levels of risk and look for innovation, in relation to its policy development and delivery outcomes where the potential rewards may provide improvements to the health and well-being of the Australian public. Conversely, the department has little to no risk appetite for engaging with risk that could harm its people or the Australian public.

#### Engagement is key

A risk aware culture provides an environment where innovation and creativity is encouraged through risk based decision making. A well defined risk appetite can assist Managers make evidence based risk decisions and support a consistent approach across the department.

Early and open conversations about risk appetite are the most important element of any risk assessment process. It is essential to understand the boundaries in which we operate and where innovation and creativity are important to achieving our strategic priorities. Risk appetite needs to be considered at all stages of our work.

#### Discuss with others:

- ▶ What level of risk are we comfortable with for each identified theme?
- ▶ Are there opportunities which have not been considered?
- ▶ Is there an alternative option which could result in a better outcome?
- ▶ How do we manage the risks with these options?
- ▶ What evidence do we have to support our decisions?

We're all responsible for having regular risk conversations and we need to ensure conversations:

- ▶ are open, straightforward and purposeful
- ▶ approach to risk management with a view to achieve set outcomes
- ▶ ensure risks are considered across all themes
- ▶ are held at all levels of the organisation as well as with external stakeholders, and
- ▶ Provide results the enable effective evidence based decision making.

#### Risk themes & scaling

The department considers risk based on where activities fall within seven core themes;



PEOPLE



FRAUD



POLICY



DELIVERY



GOVERNANCE



REGULATORY



INFORMATION

The appetite for risk changes between and within each core theme based on the business function, potential for reward and any considerations. The business scenario examples below provide guidance on each of the seven themes risk appetite levels as accepted by the department.

#### Risk appetite scale

CONTROLLED (little-to-none)	CAUTIOUS (low)	ACCEPTING (medium)	OPEN (high)
Avoidance of risk and uncertainty is a key objective	Prefer safe options with little risk of adverse exposure for department and/or the government	Willing to consider all options and choose the one that is most likely to result in successful delivery while also providing a reasonable degree of protection from high risks	Eager to engage with risks and opportunities when the potential benefit is great

#### Theme Business scenario

 PEOPLE	<b>GENERAL</b>  Activities which may put the physical or mental health of our staff or the public in danger Potentially unsafe environments requiring additional considerations to mitigate the risks as much as possible
 FRAUD	<b>GENERAL</b>  Mismanagement of information potentially creating opportunity for fraudulent activity Automating processes to provide efficiencies while accepting some risk
 POLICY	 Decisions regarding policy relating to sensitive topics Linking and proactively using information to create evidence based and innovative policy
 DELIVERY	<b>GENERAL</b>  Increased monitoring to ensure the effectiveness of our delivery mechanisms Seeking advice from external subject matter experts
 GOVERNANCE	<b>GENERAL</b>  Effective committee structures that ensure appropriate oversight of strategic alignment Delegating decision making and responsibility to build capability and streamline work
 REGULATORY	<b>GENERAL</b>  Protection of the health and safety of the Community Implementing best practice to reduce excessive burden on business and healthcare professionals and consumers
 INFORMATION	<b>GENERAL</b>  Unauthorised access to personal data Expanding data analytics capability to improve evidence based business decisions

