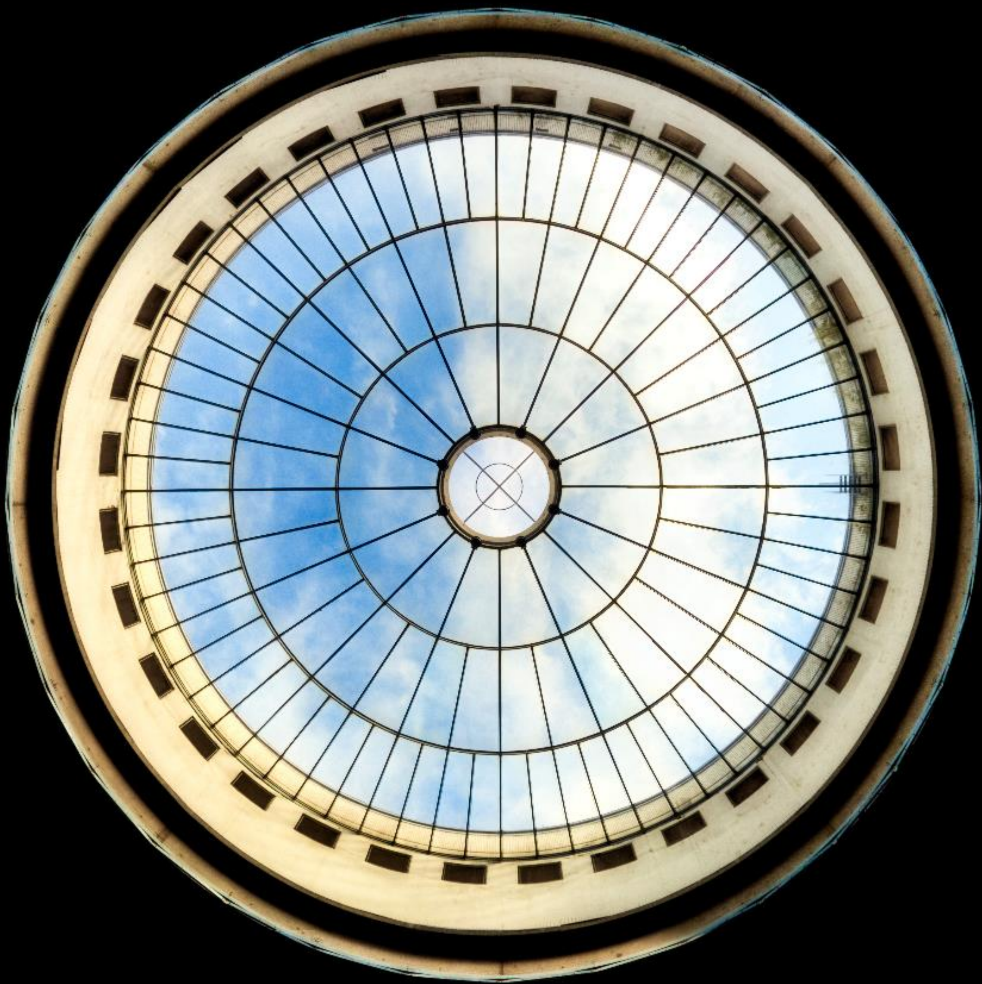


Comcover
Risk Management Benchmarking Program 2017: Key Findings Report
August 2017

Contents

Inherent Limitations

The Services provided are advisory in nature and have not been conducted in accordance with the standards issued by the Australian Auditing and Assurance Standards Board and consequently no opinions or conclusions under these standards are expressed.

Because of the inherent limitations of any internal control structure, it is possible that errors or irregularities may occur and not be detected. The matters raised in this report are only those which came to our attention during the course of performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made.

Our work is performed on a sample basis; we cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud.

Any projection of the evaluation of the control procedures to future periods is subject to the risk that the systems may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

Recommendations and suggestions for improvement should be assessed by management for their full commercial impact before they are implemented.

We believe that the statements made in this report are accurate, but no warranty of completeness, accuracy, or reliability is given in relation to the statements and representations made by, and the information and documentation provided by Comcover personnel. We have not attempted to verify these sources independently unless otherwise noted within the report.

Limitation of Use

This report is intended solely for the information and internal use of Comcover in accordance with our letter of engagement of 18 June 2014, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this report. We do not accept or assume responsibility to anyone other than Comcover for our work, for this report, or for any reliance which may be placed on this report by any party other than Comcover.

Deloitte.

Deloitte Touche Tohmatsu
ABN 74 490 121 060

550 Bourke Street
Melbourne VIC 3000
GPO Box 78
Melbourne VIC 3001 Australia

Tel: +61 3 9671 7000
Fax: +61 9671 7001
www.deloitte.com.au

Tracie-Ann Maher
Director - Risk Management Services
Risk, Insurance and Special Claims Branch
Department of Finance
One Canberra Avenue
Forrest ACT 2603

25 August 2017

Dear Tracie-Ann

Re: Risk Management Benchmarking Program – 2017 Key Findings Report

We are pleased to provide Comcover with our observations in relation to the key findings of the 2017 Risk Management Benchmarking Survey.

Should you have any questions or comments, please do not hesitate to contact me on (03) 9671 7261.

Yours sincerely

Matthew Fraser
Partner
Deloitte Touche Tohmatsu

Executive summary

1 Executive summary

1.1 Program overview

This report allows Comcover to measure capability and understand risk management performance of its participating Fund Members against the Commonwealth Risk Management Policy (the Policy).

The Risk Management Benchmarking Program (the Program) measures Fund Members' risk management maturity across the following nine elements of the Policy:

Element 1 **Establishing a risk management policy**	**Element 2** **Establishing a risk management framework**	**Element 3** **Defining responsibility for managing risk**
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**

The Program is based on a six state maturity model, as illustrated below:

Fundamental	**Developed**	**Systematic**	**Integrated**	**Advanced**	**Optimal**

These six maturity states are described, for each of the nine elements of the Policy, at: http://www.finance.gov.au/sites/default/files/rm-capability-maturity-levels-2017.docx.

1.1.1 Participants and results

The Risk Management Benchmarking Survey (the Survey) was completed by 146 General Government Sector entities in 2017. This year, the average overall maturity state across the Fund was once again integrated – indicating there is still scope to improve risk management capabilities further over the next few years. It is positive to note that the average overall risk management maturity of the Fund continues to increase in each year of the Program. Unlike in 2016, where average maturity for every element increased significantly, there were only minor increases in element level maturity this year, and some elements saw a slight decrease in average maturity. As it is the third year of the Program, this levelling of results may be explained by entities having now established solid foundational elements of their risk function, and now looking to enhance maturity in the more complex elements. Understandably, elements relating to concepts such as risk culture and shared risk management may take significantly longer for entities to address.

The survey results indicate that the highest scoring elements across the population in descending order are the same as those identified in the last two years, which were:

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

The results indicate that, on average, entities continue to score higher in those elements which represent foundational risk management concepts, including the following characteristics:

- Entities' risk management policies and frameworks are well developed, linked to strategy and aligned with the Policy
- Risk appetite and tolerance limits are increasingly a feature of entities' risk management frameworks
- A common definition of risk is understood throughout most entities and there are consistent practices for identifying, assessing and monitoring risks
- Responsibility for the management of risk has been assigned and clearly defined across the entity, including governance arrangements where performance is appraised.

While these elements are indeed crucial tools to help embed consistent risk management practices, there is potential for entities to focus efforts on building capability across the other elements of the Policy which are undoubtedly more complex, yet important in building true risk intelligence and longer term resilience. Due to this complexity, it is in line with expectations that the following elements were the lowest scoring elements across the population in 2017:

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

These and other key insights from this report are highlighted on the infographic in section 1.2 and summary of key findings in section 1.3.

1.1.2 Analysis approach and considerations

A number of considerations have been taken into account in analysing the results of this year's survey. These are as follows:

- 2017 is the third year of the current iteration of the benchmarking program
- It has been two years since the Belcher and Shergold Reviews on risk management and regulation, three years since the release of the Commonwealth Risk Management Policy (July 2014) and four years since the release of the *Public Governance, Performance and Accountability Act 2013*
- Risk management maturity must be fit-for-purpose, and entities do not necessarily need to strive for significantly increased maturity each year
- The level of risk management knowledge and awareness among entities has increased as a result of a heightened focus on enabling robust risk management practices across the public sector
- The Commonwealth more broadly is currently striving to better understand and manage shared risk and building a positive risk culture.

Analysis was conducted across the following factors:

- Overall maturity of the Fund
- Maturity and target maturity at the element level
- Entities' current and emerging risk priorities.

Analysis is aggregated at the overall Fund and element levels and is therefore not always definitive for individual entities.

1.2 Element trend insights

KEY ELEMENT LEVEL INSIGHTS

Element Overview

1 **Establishing a risk management policy**
Highest performing element for third consecutive year
Average maturity has continued to increase across all three years

2 **Establishing a risk management framework**
71% of entities achieved maturity states of Integrated or Advanced
Minor reduction in average maturity in 2017

3 **Defining responsibility for managing risk**
96% of entities achieved maturity states of Systematic or higher
Third highest performing element this year

4 **Embedding systematic risk management into business processes**
Second highest performing element this year
Average maturity state was Advanced across the Fund

5 **Developing a positive risk culture**
Largest positive movement in maturity of any element in 2017
Significant variability in entity maturity

6 **Communicating and consulting about risk**
More than half of the Fund achieved a maturity state of Integrated
No entities scored either Fundamental or Optimal maturity states

7 **Understanding and managing shared risk**
Entities continue to find this a complex area of risk management
Second lowest performing element with a decrease in maturity in 2017

8 **Maintaining risk management capability**
Increased maturity this year, yet remains as the lowest performing element in 2017

9 **Reviewing and continuously improving the management of risk**
No entities at the Fundamental maturity state and only six at Developed
Improvement in average maturity in 2017

1.3 Summary of key findings

Presented below is a summary of the key findings noted through our review of the survey responses this year, and the element, or elements, which they relate to. The detailed findings and other analysis is discussed in section 2 to 5 of this report.

#	Key finding	Related element(s)
1.	**Shared risk management is still an area that entities find challenging, indicated by a decline in the average maturity of Element 7 this year** While significant increases in maturity were seen across all elements in 2016, average maturity declined for Element 7 – relating to Shared Risk - in 2017. Although Shared Risk has been an area of focus of the Program and the APS more generally in recent years, it is evident that there remains a significant capability gap to be addressed. Positive responses declined in 2017 when entities were asked whether accountability for managing shared risks is clearly understood across the entity. Recent consultation with a range of APS entities regarding their interaction with Shared Risk supported these results, suggesting that a common definition of Shared Risk is not clearly understood, and this is still perceived as a 'grey area' for many entities.	Element 7
2.	**Entities continue to see finance and delivery of services or programs as the biggest sources of both current and emerging risk** Unsurprisingly, there was little change from 2016 in how entities prioritised their key current and emerging risks, indicating that entities are not identifying any major shifts in the macro environment. The number of entities rating political factors as a key source of emerging risk decreased this year, being replaced by Technology as a top emerging risk. People and stakeholder management were also a top four priority for the Fund as both current and emerging sources of risk, again unsurprising due to the complex stakeholder environment in which APS entities operate.	All elements

#	Key finding	Related element(s)
3.	**An increase in risk management training and investment is driving an uplift in capability, but must be reinforced outside of this to drive desired behaviours in the longer term** Despite being the lowest performing element in 2017, Element 8 - Maintaining Risk Management Capability - recorded the second largest increase in average maturity this year. Upon closer analysis, this appears to have been driven mainly by an increased provision of risk management training, with employees across all levels of the entity seeing an increase in training offerings compared with 2016. Of these, the most sizeable increase was seen in training delivered to the Chief Risk Officer and control owners. In addition, greater investment in resources such as information management systems has contributed to the enhancement in risk management capability. While it is promising to note these improvements, there is scope to complement these core programs with reinforcements to drive longer term capability uplift, such as recognition and rewards programs, risk management fact sheets and skills analyses across teams. With the greatest variance between actual and target maturity of all elements, entities will likely be looking for ways to close this gap further in the coming year.	Element 8
4.	**Proportional changes in maturity have eased in the third year of the Program as, having largely addressed foundational elements, entities now focus on the more complex elements of the Policy** Unlike the considerable increases observed in average maturity between 2015 and 2016, the magnitude of increases in average maturity for each element have plateaued in 2017, and even gone slightly backwards for some elements (including elements 2, 7 and 9). While the significant increases seen previously would not have been expected in the third year of the Program, it is important that entities do not become complacent in their approach to risk management and continue investing in their risk management capability in line with evolving external conditions. Particularly where variances remain between target and actual maturity states, it would be hoped and expected that entities would be able to make greater progress in uplifting their risk program in a 12 month period, rather than remaining stagnant and observing the same shortfalls year on year.	All elements

#	Key finding	Related element(s)
5.	**While there are still opportunities for improvement, entities are making progress in understanding how to build a positive risk culture** Element 5 recorded the largest improvement in average maturity in 2017. This is a positive result given that Risk Culture was highlighted by many entities in 2016 as an area requiring improvement, through setting of aspirational target states and post-Survey entity discussions regarding key challenges going forward. It is encouraging that entities are now responding to the direction of many of their Accountable Authorities and Audit and Risk Committees to explicitly focus on creating an environment that is conducive to robust risk management. This is a shift that will take incremental efforts over time – a more complex, long-term maturity build than that of the foundational elements such as setting the risk management policy and framework.	Element 5
6.	**Target maturity states are increasing disproportionately with actual maturity states, indicating a potential misunderstanding of a fit-for-purpose target state** The selection of higher, yet realistic, target states is appropriate and indicates the desire of entities to continually improve and invest effort and resources to drive better risk management outcomes. However, while entities appear to be aiming higher year on year, their rate of actual progress is not reflecting an apparent desire to improve in many areas. For example, Element 9 – Reviewing and Continuously Improving the Management of Risk - had the largest increase in average target maturity this year, however was one of the three elements that saw a reduction in actual maturity in 2017. This misalignment potentially highlights either, or a combination of: (i) a misunderstanding of the purpose of the target state, which is supposed to be fit-for-purpose for the entity, or, (ii) as indicated previously, a relative slowing of investment in risk management capability.	All elements

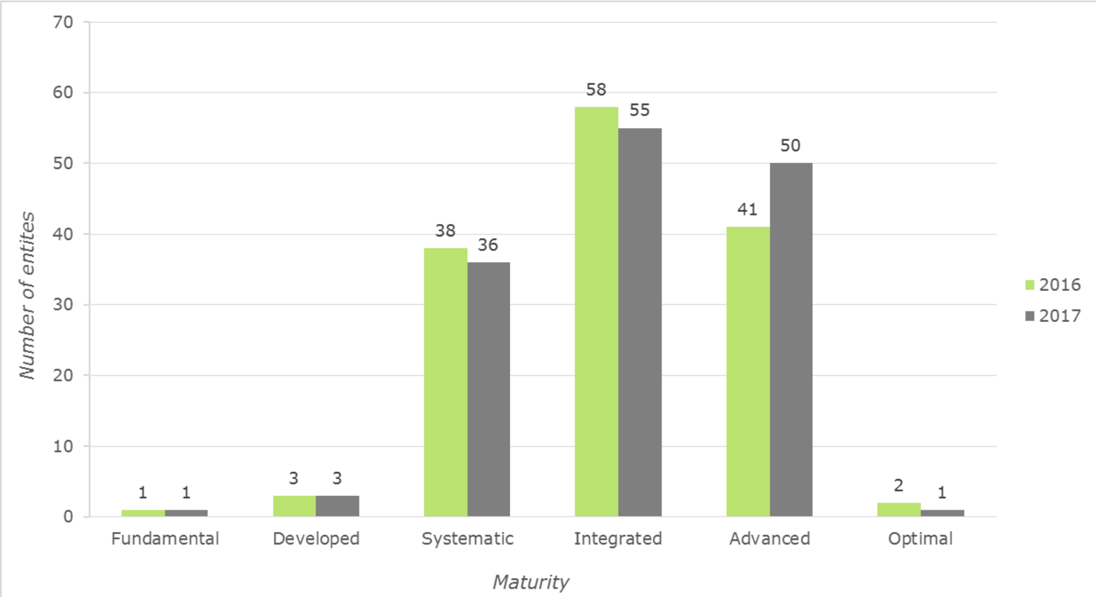
Overall Fund findings

2 Overall Fund findings

2.1 Overall performance of Fund

2.1.1 Maturity distribution

Graph 1 – Distribution of maturity levels achieved by participants overall



This year's Program saw 62% of entities achieving a risk maturity state of Systematic or Integrated, and 35% of entities achieving Advanced or Optimal maturity. These results indicate that a significant number of entities continue to align their risk management practices with the Policy.

Overall, these results show another upwards shift in maturity across the Fund, although this year's shift is far less pronounced than that seen between 2015 and 2016. The proportion of entities at the Systematic and Integrated maturity states reduced from 67% in 2016 to 62% in 2017, with more entities shifting into the Advanced maturity state. This indicates that many entities have made positive, albeit minor, progress in building their risk management capability over the last year. These results once again align to the Program's objectives – assisting entities to continuously improve their practices in order to remain resilient in a rapidly changing risk environment, and focus efforts on reaching target maturity where they may have fallen short.

2.1.2 Key operational factors

Analysis of a range of key operational characteristics of entities illustrates that the Fund is extremely diverse. Analysis of average figures shows a positive correlation between average maturity state and indicators of entity size - budgeted income, number of employees and value of assets. The exception to this correlation is at the Optimal maturity state, which can be explained by the fact that only one entity reached this category in 2017.

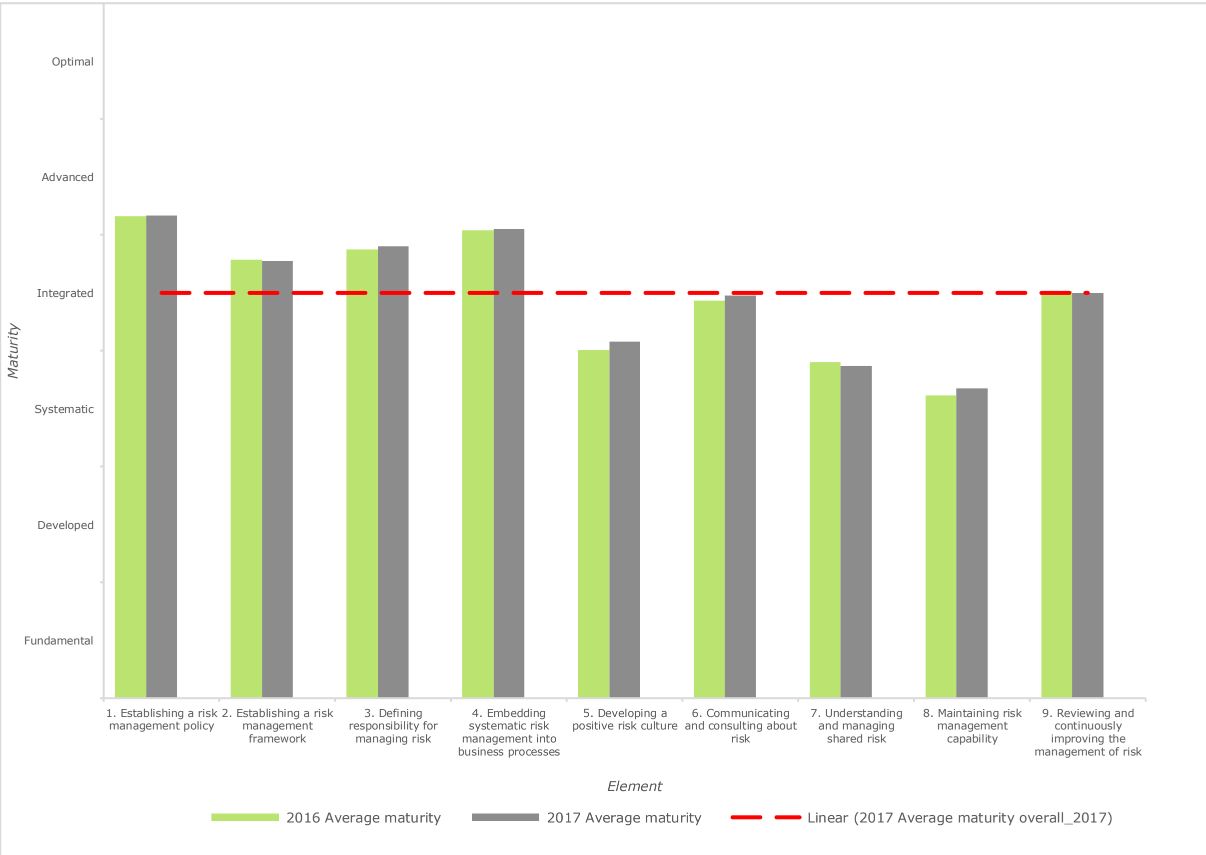
Risk management capability should be commensurate with an entity's risk exposure, regardless of how large an entity is. As such, while there appears to be a correlation between size and risk management maturity generally, size is only one factor that contributes to the complexity of an entity's risk landscape, and therefore the capability required to manage this.

2.2 Maturity across the survey elements

2.2.1 Risk management capabilities

Once again, elements 1, 3 and 4 were the highest performing elements in 2017, while elements 5, 7 and 8 were the lowest. Unlike in 2016, where there was significant improvement in the average maturity of all elements, the 2017 results indicate that improvement in maturity across all elements has eased. While it was positive to see the Fund increasing significantly in maturity from 2015 to 2016, it is acknowledged that risk maturity should be fit-for-purpose – which will not necessarily be the highest maturity for every entity. While changes in the third year of the Survey were not anticipated to be as significant, it was surprising to see that this year three elements actually saw a minor decrease in average maturity.

Graph 2 – Performance of Fund across each element



Areas of strength

Elements 1 to 4 represent the foundational elements of risk management, so it is unsurprising to see these as the strongest performing in 2017, scoring above the average overall maturity in each instance. Given the importance of these elements in setting and communicating the entity's desired risk management practices, it is encouraging to see most entities are putting these mechanisms in place to ensure that they are poised to engage with more complex aspects of risk management over time, such as those measured in elements 5 to 9.

Opportunities for improvement

As in the last two years, elements 5, 7 and 8 were the lowest performing elements - covering risk culture, shared risk and risk management capability respectively.

Given this trend, it is clear that these elements are areas of risk management that entities continue to find more challenging to implement. Acknowledgement in prior years that these are the areas in which entities continue to fall short of their targets may have contributed to improvement efforts over the past 12 months which saw an increase in the related elements this year (5 and 8) - the greatest improvement in average maturity of any elements this year. Despite this increase, Comcover and entities are encouraged to continue to build on these aspects of risk management given average maturity states remain low. Another element seeing a slight decline in average maturity in 2017 was shared risk - highlighting an area of difficulty which is becoming even more challenging for entities to manage in the absence of a clear definition and better practice examples to leverage. There exists an opportunity to agree and communicate a practical definition of shared risk, so entities can seek to better manage their complex, interdependent risks.

2.3 Risk management capabilities – element state analysis

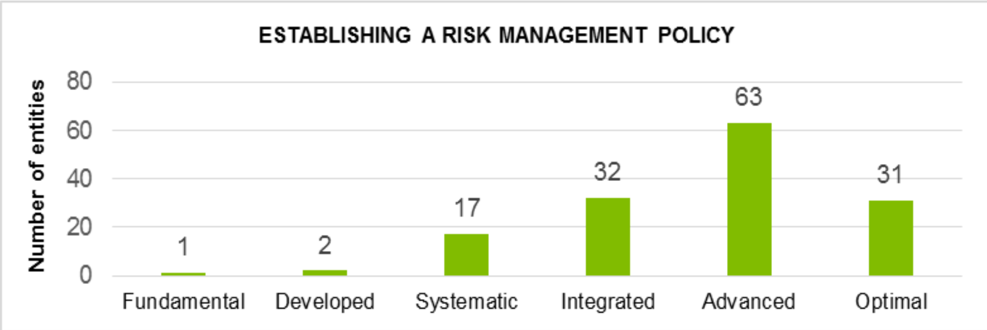
2.3.1 Element 1 – Establishing a risk management policy

Definition and context

An entity's risk management policy links the entity's risk management framework to its strategic objectives. Communicating the principles, objectives, accountabilities, responsibilities and expectations of how risk is to be managed in an entity's risk management policy is important to ensure a common understanding and application across the entity. It is important to consider risk appetite and tolerance in a risk management policy, as it provides guidance on how much risk officials can take and empowers them to make considered and appropriate risk-based decisions.

The Policy, effective from 1 July 2014, references Section 16 of the PGPA Act, which requires accountable authorities of Commonwealth entities to establish and maintain appropriate systems of risk oversight, management and internal control. For the majority of entities (92%), the risk management policy has been endorsed by the entity's accountable authority. This is a positive outcome as it indicates acknowledgement and alignment to the Policy by entities; however, as the PGPA Act mandates this, Comcover should focus on ensuring the remainder of entities have risk management policies endorsed by their accountable authority.

Analysis overview



As in the past two years, Element 1 continues to be the highest performing element across the Fund, with 64% of entities scoring within the two highest maturity states, and more entities reaching Optimal (21%) than in any other element. This indicates that many entities have established risk management policies which include important components and attributes in line with better practice guidance.

Response drill-down

Key structural policy elements are generally included in entities' risk management policy documents. Almost all entities (i.e. greater than 95%) agreed that their risk management policy includes the objective and scope of the policy, accountabilities and responsibilities for managing risk, and their approach and rationale for managing risk.

A considerable number of entities have also aligned their risk management policies with relevant better practice standards (84%) and received endorsement from the entity's accountable authority (92%).

This year, there was a notable improvement in the number of entities communicating the entity's vision for risk management through the policy – with 82% of entities having incorporated this in 2017, compared with only 68% in 2016. The majority of entities (79%) also included a clear link between risk management and the entity's objectives in their policy, highlighting the importance of robust risk management in achieving positive outcomes, rather than being seen as a negative activity.

Risk appetite continues to be a concept defined by the vast majority of entities, with only 3% of entities responding that they have not defined their risk appetite. Importantly, an increasing number of entities are using risk appetite to inform policy, program and / or project decisions (82%), as well as to inform strategic planning (77%). In addition, 71% of entities use risk appetite as a tool to optimise the design and efficiency of controls by highlighting priority areas for risk mitigation.

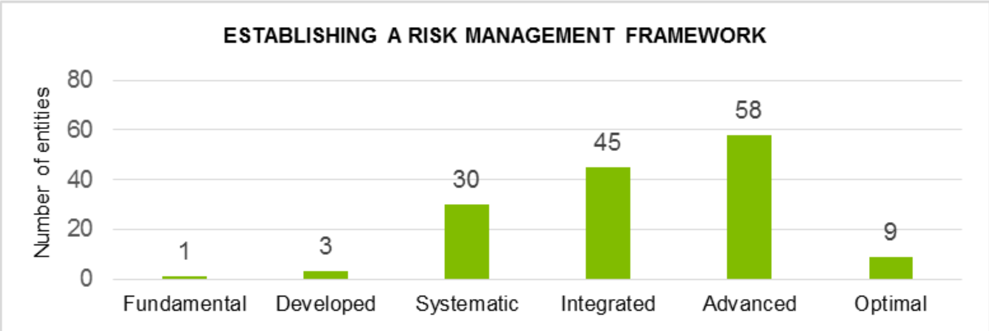
Whilst it is positive to note that risk appetite is increasingly informing strategic activity, opportunity exists for many entities to explicitly document their risk appetite, as almost a quarter of entities still have not incorporated this into their framework (23%). More entities may also benefit from defining risk appetite at the risk category level, as over a third of entities do not have category-level risk appetite statements (36%). In the absence of risk appetite which is set at the category level, its usefulness may be hindered due to being too high-level for practical application throughout the entity.

2.3.2 Element 2 – Establishing a risk management framework

Definition and context

A risk management framework is the set of components and arrangements that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the entity. It is important for a risk management framework to be suited to the purpose, structure and size of an entity, and to be aligned with key business planning, management and decision-making processes.

Analysis overview



Element 2, a key foundational element of risk management, is once again among the highest performing elements in 2017. The average maturity achieved in 2017 was Integrated, with a large number of entities (71%) achieving maturity states of either Integrated or Advanced.

These results indicate that many entities continue to support their risk program through a comprehensive risk management framework which encourages consistency of process and approach across the entity. However, while average maturity remains at Integrated in 2017, there was a minor reduction in the average actual score achieved.

Response drill-down

When asked about the components of their respective risk management frameworks, the vast majority of entities confirmed the inclusion of the following core elements:

- Documentation of roles and expectations of officials to manage risks (91%)
- Risk management methodology (90%) and context (84%)
- Outline of risk governance structure and accountabilities (92%)
- Monitoring and review requirements (89%)
- Risk related reporting requirements (82%).

Importantly, this translated well into practical application of the framework, with many entities (75%) confirming that their framework is consistently applied across all or most business units, processes, services and projects. To ensure the risk framework remains current and relevant, the majority of entities review their risk management framework at least annually (65%).

Survey responses also indicated that entities were proficient in capturing key risk information when identifying risks, such as current controls and their effectiveness (92%), potential consequences (97%) and mitigation strategies (98%).

However, when identifying risks, a smaller portion of entities considered more sophisticated risk concepts, such as relevant Key Risk Indicators or metrics which would trigger escalation (49%) and the link between the risk and the entity's strategic objectives (63%).

The majority of entities continue to report on standard risk information to interested parties across the entity, with responses indicating that risk reporting commonly includes the following information:

- Current strategic risks (91%)
- Current operational risks by line area / business unit / function (84%)
- Current project / program risks (86%)
- Status of treatment plans / action plans (77%).

However, future and emerging risks are only reported by 68% of entities, and shared risks are only reported by 40%, indicating that these important sources of risk still do not receive high visibility across a large proportion of the Fund.

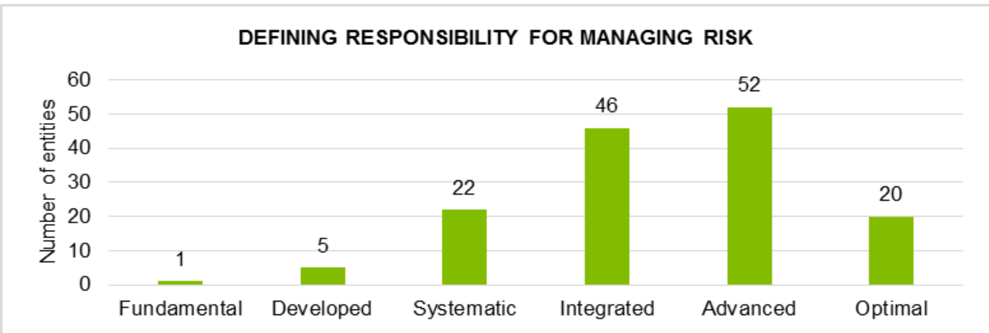
2.3.3 Element 3 – Defining responsibility for managing risk

Definition and context

The Policy requires an entity's accountable authority to allocate responsibility for determining the entity's appetite and tolerance for risk, implementing the entity's risk management framework and defining entity roles and responsibilities in managing individual risks.

The accountable authority of an entity is ultimately responsible for establishing appropriate systems of risk oversight and management. Determination of the entity's objectives and goals for its risk management program by the accountable authority sets the tone at the top. However, responsibility for the day-to-day management of risk lies with staff at all levels and should be clearly defined in the performance agreements and contracts of staff across the entity.

Analysis overview



Element 3 was the third highest performing element across the Fund for the third consecutive year, with an average maturity state of Integrated. As shown in the graph above, a significant proportion of entities (66%) achieved either Integrated or Advanced maturity this year. In contrast to Element 2 where there was a similar distribution across Integrated and Advanced, there are significantly more entities achieving Optimal in Element 3.

Response drill-down

The risk management policy is the key vehicle for almost all entities to define and communicate accountabilities and responsibilities for managing risk (99%). This information is also disseminated through the risk management framework for 90% of the Fund.

Risk management roles and responsibilities are also communicated through the audit or risk committee charters or terms of reference of the vast majority of entities (97%). Utilising more sophisticated methods of documenting and communicating these roles and responsibilities was less common, with only 20% of entities using a responsibility matrix (e.g. R.A.C.I) and 60% of entities having identified and documented control owners.

A significant proportion of entities have explicitly defined core, senior roles and responsibilities for managing risk, such as audit committees (97%), senior management (96%) and accountable authorities. However, entities are less likely to have defined and documented more specialised risk roles, such as risk managers (66%) and risk committees (53%). Opportunity exists for entities to strengthen their risk management platform by formalising and documenting these important risk management roles and responsibilities, where resources permit and the roles exist in practice.

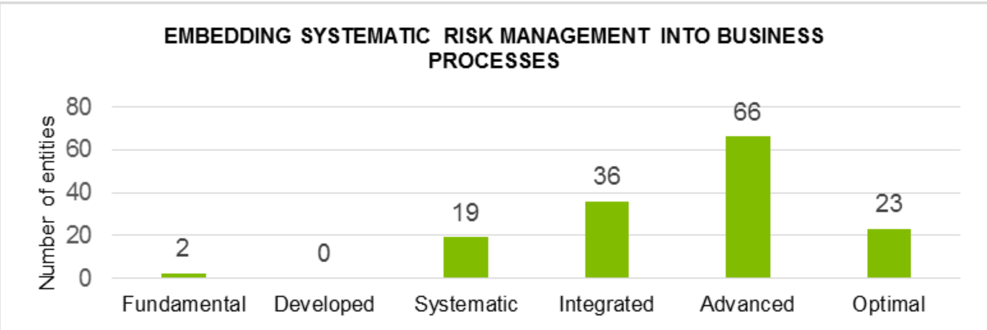
As in the last two years, only a quarter of entities have a risk function solely or primarily dedicated to the management of risk (25%). In the absence of a sole risk function, entities more commonly utilise shared risk functions, responsible for both risk and non-risk management activities (45%). This is an important consideration in interpreting entity results across other elements, as the absence of a dedicated risk function and associated resources can inherently limit the risk management maturity able to be achieved by an entity.

2.3.4 Element 4 – Embedding systematic risk management into business processes

Definition and context

The goal of the Policy is to embed risk management into key business processes such as: strategic planning; the establishment of governance arrangements; policy development and program delivery, in order to drive more informed entity-wide decision making. Successfully embedding risk management requires a tailored approach to align the entity's objectives, risk management framework and its operating environment. In our experience, the approach taken by entities is prioritised and gradual in order to demonstrate the value, build culture and target specific areas in larger, more complex entities.

Analysis overview



As in the past two years, Element 4 remains the second highest performing element in 2017, indicating that a large proportion of entities believe that their risk management framework is applied to a range of operational and strategic processes. Continued strong performance in this element represents a level of optimism among entities in the day-to-day application of the framework by staff and management, however the measures in place for entities to ascertain this level of comfort are less clear. The average maturity state

achieved in 2017 was Advanced, and more than half of entities (58%) achieved either Advanced or Optimal maturity in this element. As shown in the graph above, only a very small proportion of entities sit within the three lowest maturity states, which suggests that many entities successfully embed risk management into all key business processes.

Response drill-down

A broad range of formal mechanisms are employed across the Fund to help build and maintain organisational resilience. Almost all entities have business continuity plans (95%) and disaster recovery plans (93%) in place, demonstrating a slight improvement since 2016. Performance management is another mechanism used by the vast majority of entities to support organisational resilience (95%).

In addition to the use of broad resilience mechanisms, entities also scored well when asked about the application of their risk management processes to specialist categories of risk. For example, both fraud control and work health and safety processes are aligned with the overarching risk management framework in over 92% of entities – demonstrating that the framework has been embedded into more operational areas.

In embedding more advanced risk management techniques into business processes, such as quantitative risk analysis, results were lower across the Fund. While a quarter of entities acknowledged not using any quantitative risk analysis techniques at all, of the entities that do perform this analysis, the following areas featured most commonly:

- Finance, credit and / or tax (63%)
- Projects and programs (55%)
- Work health and safety (51%)
- Asset management (45%).

This year, improvement was noted in the use of risk categories for assessing and reporting on risk. In 2017, 73% of entities reported that they use risk categories to facilitate the efficient allocation of resources, compared with only 59% in 2016. Risk categories were also used to facilitate more effective risk reporting (82%) and to increase efficiency in risk assessment processes (89%) - both marginal improvements on last year's results.

2.3.5 Element 5 – Developing a positive risk management culture

Definition and context

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 approach to managing risk that considers both threat and opportunity.

Risk culture is closely linked to the foundational risk management elements of establishing a risk management policy and framework; defining responsibility for managing risk and effectively embedding systematic risk management into business processes. If they are implemented well, the risk culture ofan entity will be enhanced.

Analysis overview

Element 5 was once again among the three lowest performing elements in 2017. Acknowledging that building a positive risk culture is an iterative process and will not be achieved through any individual change, it is expected that entities will continue to demonstrate incremental improvements in this element over time. Despite an average maturity state at the lower end of Integrated in 2017, it was positive to note that the average score has increased since last year. Risk culture saw the largest positive shift in maturity of any element in 2017 – an encouraging outcome possibly reflecting the increasing focus of Senior Executives and Audit or Risk Committees on understanding their entity's risk culture.

As in 2016, results show significant variability in entity maturity for Element 5. This year, 91% of entities fell between the Developed and Advanced maturity states, with a relatively even representation of 20-25% of entities in each of these states.

Response drill-down

Risk culture is being led from the top in most entities, with primary responsibility for defining the entity's risk culture lying with the accountable authority for the majority of the Fund (78%).

The area responsible for conducting risk culture assessments was less consistent across the Fund, with a third of entities using their risk function (32%), and a quarter of entities conducting assessments through either internal audit (16%) or human resources (9%). However, it is important to note that only 37% of entities assess their risk culture at least annually, and almost a third of entities (32%) do not actively assess risk culture.

Of entities that do conduct risk culture assessments, the main techniques employed included data analysis from existing data sources (50%), focus groups or workshops (43%) and individual interviews (40%) - reflecting the importance of qualitative information in measuring risk culture.

Risk culture is also a product of embedding robust risk management practices at all levels of the entity, to communicate the importance of every individual's role in managing risk.

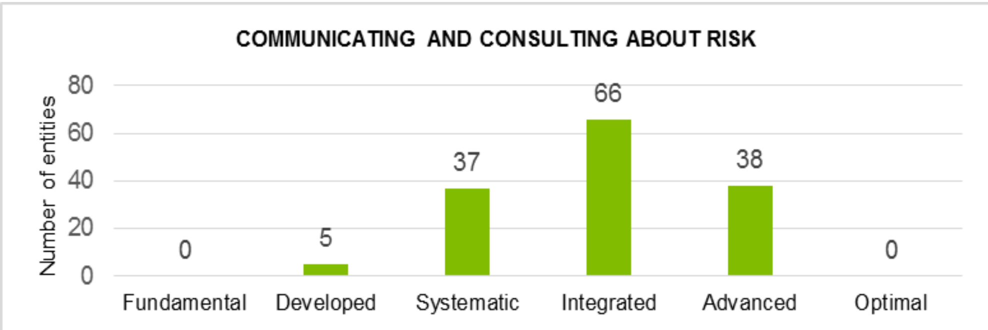
As such, it was positive to see that risk management training is provided to the majority of executive level staff (74%), senior executive level staff (70%), and APS level staff (70%). However, as a positive risk culture is built from engagement at all levels, it is also important for more junior staff to be exposed to risk management as early as possible. Despite a slight increase on last year's results, the proportion of graduate level staff receiving risk training is still low, at only approximately a third of the Fund (37%).

2.3.6 Element 6 – Communicating and consulting about risk

Definition and context

Communicating and consulting about risk underpins the successful management of risk. Effective communication requires consultation with relevant stakeholders and the transparent, complete and timely flow of information between decision makers. Communicating risk information with stakeholders is important, as it maintains confidence and trust and develops a common understanding of the entity's risks. Guidance on implementing the Policy suggests that external stakeholders such as ministers, other government entities, suppliers and the wider community may need an opportunity to communicate their views and feel involved in decision making where appropriate.

Analysis overview



As shown in the graph above, nearly half of the Fund (45%) achieved a maturity state of Integrated for Element 6 in 2017. With almost all entities (97%) scoring between Systematic and Advanced maturity for Element 6, there appear to be well established systems to share risk information throughout most entities – a key enabler in effective risk management.

In contrast to the spread of maturity across other elements, there were no entities who scored at either the highest or lowest maturity states for Element 6. This highlights that, while all entities communicate about risk to some extent, there is also more that can be done to enhance communication for many entities, particularly those with complex risk profiles and stakeholder groups. We would hope to see a greater number of entities at the Advanced and Optimal maturity states in future years as regular, open and transparent dialogue within and between entities becomes an increasingly important tool for managing complex and shared risks, and sharing learnings across the APS.

Response drill-down

Most entities encourage accountability through communicating, at a high level, core risk management roles and responsibilities through their Audit or Risk Committee Charter or Terms of Reference (97%) and their risk management policy (90%).

In keeping interested stakeholders informed, many entities formally communicate and share risk information at least every six months with their Audit or Risk Committees (90%), senior management as risk owners (69%), or in periodic business unit or divisional meetings (65%).

The information communicated in these forums and through regular risk reporting is common across the Fund, with current strategic risks (91%), current project or program risks (86%) and current operational risks by business unit or function (84%) all reported by most entities. However, it is less common for Fund Members to incorporate advanced risk concepts into their risk reporting such as key risk indicators (46%), shared risks (40%) and loss event or near miss data (38%). While an entity's suite of risk reports needs to be fit-for-purpose and easy to interpret, there is room for many entities to include these more pre-emptive or 'lead' indicators in risk reporting, as they ultimately enable an entity to act prior to a risk materialising.

Information sharing with parties external to the entity has improved slightly this year, with more than three quarters of entities (77%) now sharing risk information with other entities on an ad hoc basis. Particularly within an entity's own Community of Practice, there is a great deal that can be learnt from sharing both positive and negative risk management outcomes with other entities and, while entities are increasingly open to these forums, ideally more entities should be sharing information at least periodically.

2.3.7 Element 7 – Understanding and managing shared risk

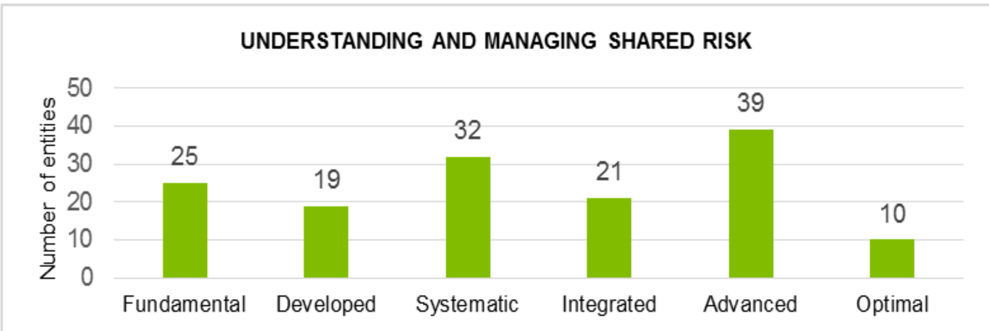
Definition and context

Shared risks are those risks 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, community, industry or other jurisdictions.

Understanding and managing shared risk is important for effective policy and program design and implementation. It is important to consider all relevant external parties that may be involved in, or influence, risk management within entities.

As government is now more interconnected, effective management of shared risk allows entities to clarify accountabilities for those risks with wide-spread causes and consequences. Such collaboration allows better practices and experiences to be shared and valuable insights to be leveraged.

Analysis overview



As the second lowest scoring element in 2017, results indicate that shared risk is a concept that many entities continue to find complex, or do not consider at all as part of their risk management program. As in Element 5, Element 7 saw a substantial spread of entities across all maturity states. While the average maturity state in 2017 was relatively low at Systematic, it is interesting to note that 10 entities achieved Optimal maturity this year, indicating that some entities appear to excel in what is undoubtedly a complex area of risk management. This finding potentially highlights some case studies which could be shared across the APS, particularly with Element 7 having four times the number of entities at the Fundamental state than any other element. Recent consultation with a

selection of APS entities regarding shared risk suggests that there is still a lack of clarity around the true definition of a shared risk, and this may lead to a reluctance to recognise shared risk all together.

As experience suggests that most, if not all, APS entities are exposed to a level of external dependencies influencing their risk profile, it is clear that there is scope for many entities to employ more systematic identification processes to consider where shared risks may exist for them.

Response drill-down

Unfortunately, the proportion of entities that do not proactively identify inter-entity shared risks at all increased from 6% in 2016 to 13% in 2017, and entities that have defined accountability for managing shared risk reduced from 41% to 38% of entities in 2017. These results have contributed to an overall decrease in average maturity in this element, despite shared risk being an area of focus in last year's report and a focus across the APS more generally.

Of entities that do seek to identify their shared risks, senior management teams (79%) and project managers (64%) were most commonly seen as responsible for driving the exercise. Methods of identification were predominately through senior management meetings and forums such as the Secretaries Board or APS 200 (62%), analysis of operational or functional risk registers (60%) and environmental scans (43%).

For those entities whose risk identification exercises did uncover shared risks to then be managed, the most common ways to do so were:

- Senior management oversight (71%)
- Organisational working groups or committees (57%)
- A Memorandum of Understanding (MoU) between the entity and other entities (56%).

Due to the complex nature of effectively managing shared risk with external parties, information sharing is critical, however shared risk is not a regular fixture in the risk reports of many entities. Most entities (55%) report on shared risks only on an ad hoc basis, 28% of entities report on shared risks approximately every 6 months, and 11% of entities indicated that shared risks are not reported to senior management at all. Given the recent focus of the ANAO and therefore senior management on shared risk, it is expected that, going forward, greater transparency over shared risk management will be required and periodic reporting would naturally be a key tool to facilitate this. However, it is also acknowledged that many entities are not yet at the stage of reporting shared risk due to not having first been through a true identification exercise on which to report against.

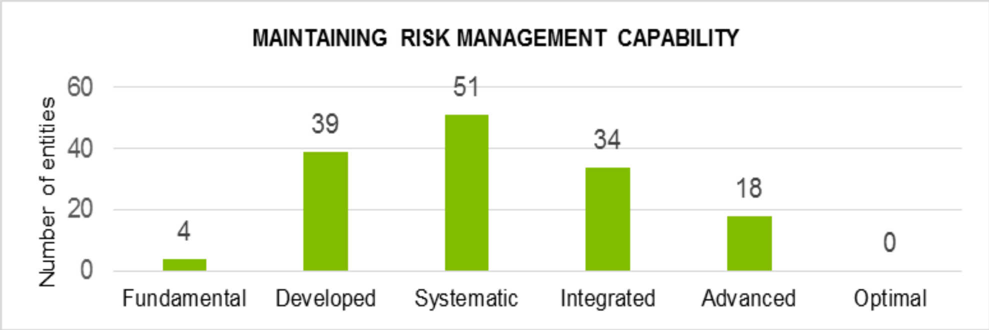
2.3.8 Element 8 – Maintaining risk management capability

Definition and context

Risk management capability refers to risk systems, tools and skills including the experience of people in the entity and the ability of the entity to manage its risk information and build effective risk management processes.

Effective risk management requires an entity to maintain an appropriate level of capability to manage its risk management program and its risks. The nature and scale of this capability must be considered in the context of an entity's current resource and capability profile and be commensurate with the characteristics and complexity of its risk profile.

Analysis overview



Element 8 - Maintaining Risk Management Capability - was once again the lowest performing element in 2017. The graph above clearly shows results skewed towards the lower end of the maturity scale, with an average maturity state of Systematic where more than a third of entities sit. 85% of entities were in the range of Developed to Integrated maturity states, and no entities achieved Optimal this year.

Despite registering the lowest average maturity across all elements, it is positive to note that this element saw the second largest increase in average maturity from 2016. As in another area of similarly low maturity – risk culture - it is positive to see that entities have acknowledged the continuing shortfall against target states and appear to be implementing initiatives which seek to build risk management capability.

Response drill-down

It is apparent that entities continue to focus efforts on building risk management capability through more senior members of the organisation. Training is most commonly provided to executive level staff (74%), senior executive service level staff (70%), APS level staff and project or program owners (64%). However, it was positive to note that, despite remaining relatively low in comparison, there was an increase in the proportion of graduate level staff participating in risk management training (37%) in order to drive a consistent risk management approach from the bottom up. A notable increase was also seen in the provision of risk training and development to the Chief Risk Officer - from 32% of entities in 2016 to 40% in 2017. An increased prevalence in the Chief Risk Officer role in general across the APS over the past 12 months is possibly a driver of increased performance in this element, as a clear steward for driving this capability.

Despite seeing some improvements on last year's results, there is scope to further increase the delivery of training to groups at the core of risk management such as control owners (34%), risk teams (42%), risk champions (28%) and risk managers (52%). Furthermore, 10% of entities do not provide any risk specific training to build and support the risk management capabilities of staff. While risk management capability is not built in a classroom, training certainly has a role in providing a solid foundation and equipping staff with an understanding of their own role in managing risk, and how to do so within the entity's desired approach and framework.

Emphasising the importance of real-world training in building risk management capability, entities were seen to use the following training techniques most commonly this year:

- On-the-job training (89%)
- Induction programs (71%)
- Face-to-face training sessions (68%).

It is positive to see that these common training methods are those involving knowledge sharing from other employees. Opportunity exists, however, for entities to reinforce these training sessions with supplementary materials such as risk management fact sheets (39%), online training sessions (50%) and through undertaking skills analyses to identify capability gaps within the workforce which can then be addressed (27%).

As well as building internal capability, it is important for entities to know when to invest in external support to help them better manage certain elements of their risk profile. When asked about these investments, it was unsurprising that 90% of entities utilise insurance cover to minimise risk exposure, and many entities (60%) use consultants for flexible access to specialist risk capability. Less commonly budgeted for by entities were risk management systems (28%), dedicated risk management resources (44%) and risk communication within the entity (16%).

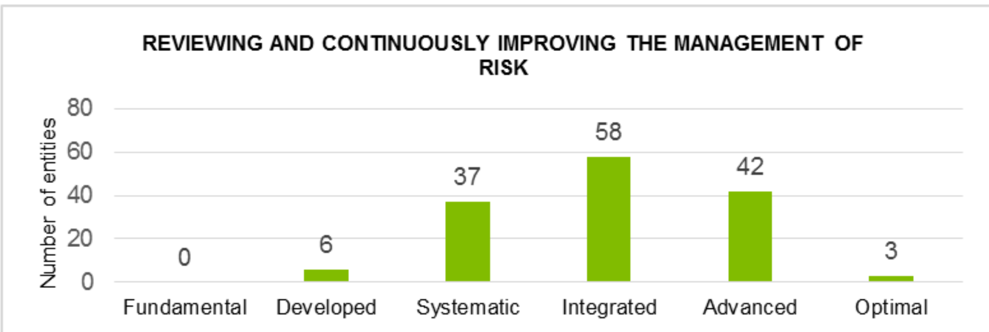
These efforts to enhance risk management capability must also be complemented by safeguarding mechanisms to maintain current capability. As with maintaining corporate knowledge in any business area, robust systems for managing risk information is core to this. Entities manage their risk information in a variety of different ways, including excel spreadsheets (51%) and file sharing platforms (22%). However, only a very small proportion of entities (8%) are currently using purpose built Governance, Risk and Compliance software or a Governance, Risk and Compliance module of their Enterprise Resource Planning system (3%). While investing in these tools will not be feasible or necessary for many smaller entities, the complexities of a large department certainly warrant exploration of a more robust information management system to not only house this information, but also to generate reports and track progress against audit findings or treatment plans.

2.3.9 Element 9 – Reviewing and continuously improving the management of risk

Definition and context

Formalising and implementing risk management within an entity is not a 'one-off event'. The effective management of risk is a process of continuous improvement, requiring regular review and evaluation mechanisms. Entities need to continuously review their risk management framework and the risks being managed so that they are equipped with the information to enable new risk identification and adjust their risk profile to make it relevant and meaningful. Effective review and evaluation mechanisms enable entities to check whether their respective approach to risk management is consistent with their objectives, while also enabling a platform to reward good performance as it links to risk management activities.

Analysis overview



Element 9 was the fifth strongest element in 2017, with an average maturity state of Integrated and almost all of the Fund (94%) with maturity between Systematic and Advanced. It is positive to note that in 2017 there were no entities at the Fundamental maturity state for Element 9, and only six entities at the Developed maturity state. These results are pleasing to see as, although to varying degrees, this indicates that all entities have at least some mechanisms in place to critically analyse their risk management performance and identify possible improvements. In line with the philosophy that standing still is essentially going backwards, these review mechanisms put entities in good stead to keep up with a continuously evolving risk landscape.

Response drill-down

Core risk artefacts such as the risk management policy and framework set the foundations for the desired risk management approach within each entity. As internal and external factors in the risk environment are constantly changing, it is important that these risk artefacts are kept relevant through regular review. Results indicate that risk management policies are reviewed and updated annually by 63% of entities and risk management frameworks by 60% of entities.

In order to ensure the entity’s most dynamic risk artefacts - their risk profiles - are current and relevant, many entities consult with the following at least annually:

- Audit or risk committees (98%)
- Senior management (96%)
- The accountable authority (92%)
- Internal subject matter experts (90%)
- Third party specialists (52%).

As well as refreshing existing risk management tools, entities should also seek to identify broader improvement opportunities in their risk management practices. It is therefore important, as in any business area, to monitor and measure performance over time to identify areas of strength and relative weakness. This year’s results indicate that entities primarily measure their risk management performance based on internal audit outcomes (90%) and the monitoring and reviewing activities of senior management or the accountable authority (85%). However, results indicated that a smaller proportion of entities benefit from utilising more pre-emptive performance monitoring techniques such as analysing quantifiable key risk indicators, currently used by only 32% of entities, and near miss analysis, used by only 39% of entities. These measures are useful in their ability to indicate potential risk management capability gaps early through trending data rather than ‘after the fact’ risk management gaps uncovered through actual failures and audit findings.

Whether or not these appraisals result in identified weaknesses in risk management performance, an outward looking focus on continuous improvement will assist entities in navigating a risk landscape which evolves and increases in complexity year on year. It is therefore positive to see that many entities are now proactively seeking better risk management practices which could enhance their own risk program. While better practice is still commonly identified through traditional audit avenues, such as ANAO outcomes (91%) or risk-specific internal audit reviews (84%), entities are increasingly seeking learnings through staff attendance at risk management networks, conferences and forums (80%), knowledge sharing between APS entities (61%) and research conducted by the entity’s risk function (61%).

Target maturity findings

3 Target maturity findings

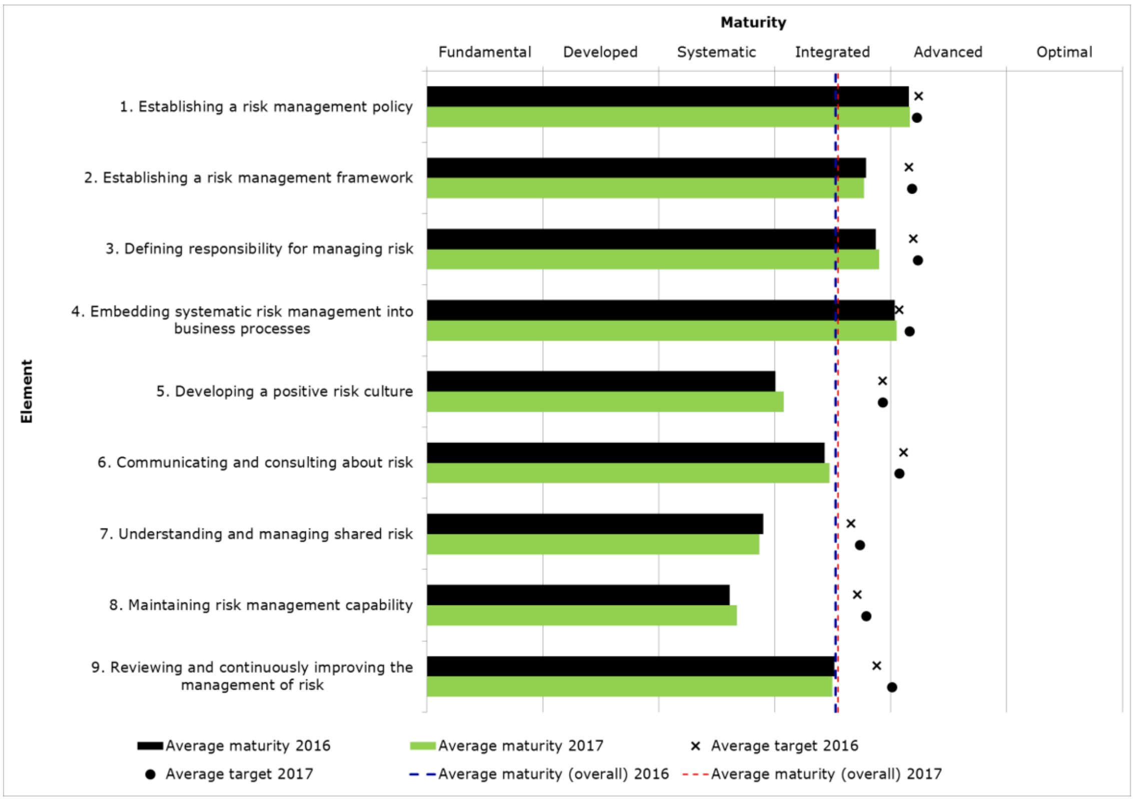
3.1 Setting target maturity states

During the survey completion process, all entities were asked to select an individual target state of risk maturity for each of the nine elements from the Policy, representing where they would like their risk management capability to be at an element level within the next 12 months.

In considering the appropriate state of risk maturity for an entity to work towards, entities are encouraged to align their investment in risk management with the needs of the entity with respect to the size, complexity, operating environment and agreed expectations of their accountable authority.

3.2 Achievement against targets

Graph 3: Comparison of current and target maturity of the total population for each element



3.2.1 Current versus target maturity states

It is interesting to note that, with three years of comparable data now available, there has only been one instance where average actual maturity for an element has met or exceeded its average target maturity. This selection of higher, yet realistic, target states is appropriate and indicates the desire to continually improve and invest effort and resources to drive better outcomes through effective risk management.

While increases were observed in the averages of both target maturity and actual maturity in 2017, these increases were both significantly smaller than those seen in 2016.

There were notable increases in target maturity in a number of elements, however these increasing aspirations were not met with similar increases in actual maturity. While entities appear to be aiming higher year on year, their actual progress is not reflecting their apparent desire to improve in many areas. For example, Element 9 – Reviewing and continuously improving the management of risk - had the largest increase in average target maturity this year, however was one of the three elements that saw a minor reduction in actual maturity in 2017.

Differences in the proportional change in target and actual maturity are depicted in graph 3 by the almost identical placement of the red and blue actual maturity lines showing 2016 versus 2017, whereas movement is much more pronounced between the target maturity markers of 2016 and 2017.

3.2.2 Entities with scores below their targets

The setting of target maturity states is designed to drive improvements in entity capabilities. As a result, we would expect targets to consistently sit above the scores entities are achieving for each element, with both figures increasing in parallel over time.

In line with this, Table 1 illustrates the number of entities that achieved maturity below the target for each element. Again, this demonstrates that the greatest area for improvement sits across Elements 5, 7 and 8. This is in line with expectations, as these were the three lowest performing elements overall. Element 7 showed considerable average variance between actual and target scores, indicating that shared risk is an area that entities continue to struggle with, with almost half of the Fund aspiring to higher maturity in this area than they have achieved. Notably, less than 20% of entities achieved maturity below their targets for elements 1 – 4.

Table 1: Distribution of achieved maturity below target for each element

Target > Actual		
Element	**Number of entities below target**	**Average of percentage difference in score**
1. Establishing a risk management policy	22	34%
2. Establishing a risk management framework	28	37%
3. Defining responsibility for managing risk	28	35%
4. Embedding systematic risk management into business processes	16	36%
5. Developing a positive risk culture	63	46%
6. Communicating and consulting about risk	43	32%
7. Understanding and managing shared risk	67	60%

8. Maintaining risk management capability	77	47%
9. Reviewing and continuously improving the management of risk	41	18%

3.2.3 Entities with scores above their targets

Table 2 illustrates the number of entities with actual scores above their target for each element. This demonstrates that the strongest area of achievement has been in elements 1, 3 and 4, with approximately half of the Fund achieving maturity above their targets for elements 1 and 4. These target results are once again aligned to the three highest performing elements in actual terms.

Table 2: Distribution of achieved maturity above target for each element

Actual > Target		
Element	**Number of entities above target**	**Average of percentage difference in score**
1. Establishing a risk management policy	73	21%
2. Establishing a risk management framework	43	12%
3. Defining responsibility for managing risk	51	16%
4. Embedding systematic risk management into business processes	70	20%
5. Developing a positive risk culture	31	18%
6. Communicating and consulting about risk	28	15%
7. Understanding and managing shared risk	44	26%
8. Maintaining risk management capability	16	17%
9. Reviewing and continuously improving the management of risk	35	25%

Where entities are achieving maturity above their target state, it is an opportunity for entities to consider refocusing effort to areas of lower capability and to reassess whether current investment in these areas is fit-for-purpose.

We recommend that Comcover focuses on target setting activities of entities to ensure they are following an appropriate process, and that entities' targets demonstrate a desire to improve their existing capabilities.

3.2.4 Entities that scored within targets

Table 3 illustrates the number of entities with actual scores equal to their target for each element. This shows that more than half of the Fund achieved their target maturity state in elements 2 and 6, with most elements seeing at least a third of the Fund achieving target states. As in other areas of results analysis, managing shared risk is again a standout lower performer from this perspective, with less than a quarter of the Fund achieving actual results that reflect where they think they need to be.

It is important that, where target maturity is achieved for any particular element, entities do not become complacent and cease to invest in continuous improvement of their capability in these areas. As the risk landscape continues to evolve each year, failure to incrementally build and enhance capability in these areas will undoubtedly see entities go backwards in actual maturity.

Table 3: Distribution of achieved maturity equal to target for each element

Actual = Target	
Element	**Number of entities achieving target**
1. Establishing a risk management policy	51
2. Establishing a risk management framework	75
3. Defining responsibility for managing risk	67
4. Embedding systematic risk management into business processes	60
5. Developing a positive risk culture	52
6. Communicating and consulting about risk	75
7. Understanding and managing shared risk	35
8. Maintaining risk management capability	53
9. Reviewing and continuously improving the management of risk	70

Current and emerging risks

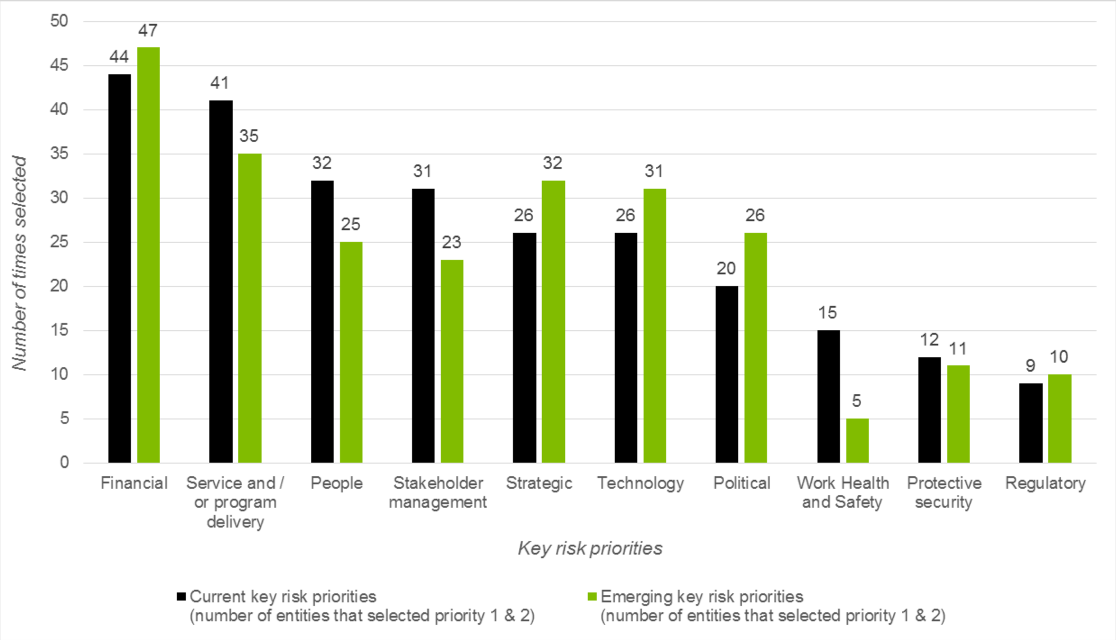
4 Current and emerging risks

4.1 Current and emerging risk priorities

As part of the Survey, entities were asked to prioritise which sources of risk are most relevant and important to their situation, both from a current and emerging perspective. Each entity selected five predetermined options and ranked these in order of importance from one (high priority) to five (low priority).

Entities appear to understand the concept of emerging risk as being different to current risk, as the prioritisation has remained slightly different each year in the two categories. Emerging risk is a perceived, yet unknown, area of risk that may eventuate in future.

Graph 4: Key risk priorities – current versus emerging sources of risk



Graph 4 summarises the most frequently nominated top 10 current and emerging sources of risk. Key risk priorities are derived from the frequency of a risk source being deemed as an entity's first or second priority.

Entities indicated that the following sources of risk were most relevant to their current risk profile:

1. Financial
2. Service and/or program delivery
3. People
4. Stakeholder management.

While the top risk sources remain relatively constant this year, it is interesting to note a slight shift from last year's top current priorities where there was greater importance placed on strategic risk - now replaced in the top four by stakeholder management.

Looking forward, entities saw the following as the most significant emerging sources of risk:

1. Financial
2. Service and/or program delivery
3. Strategic
4. Technology.

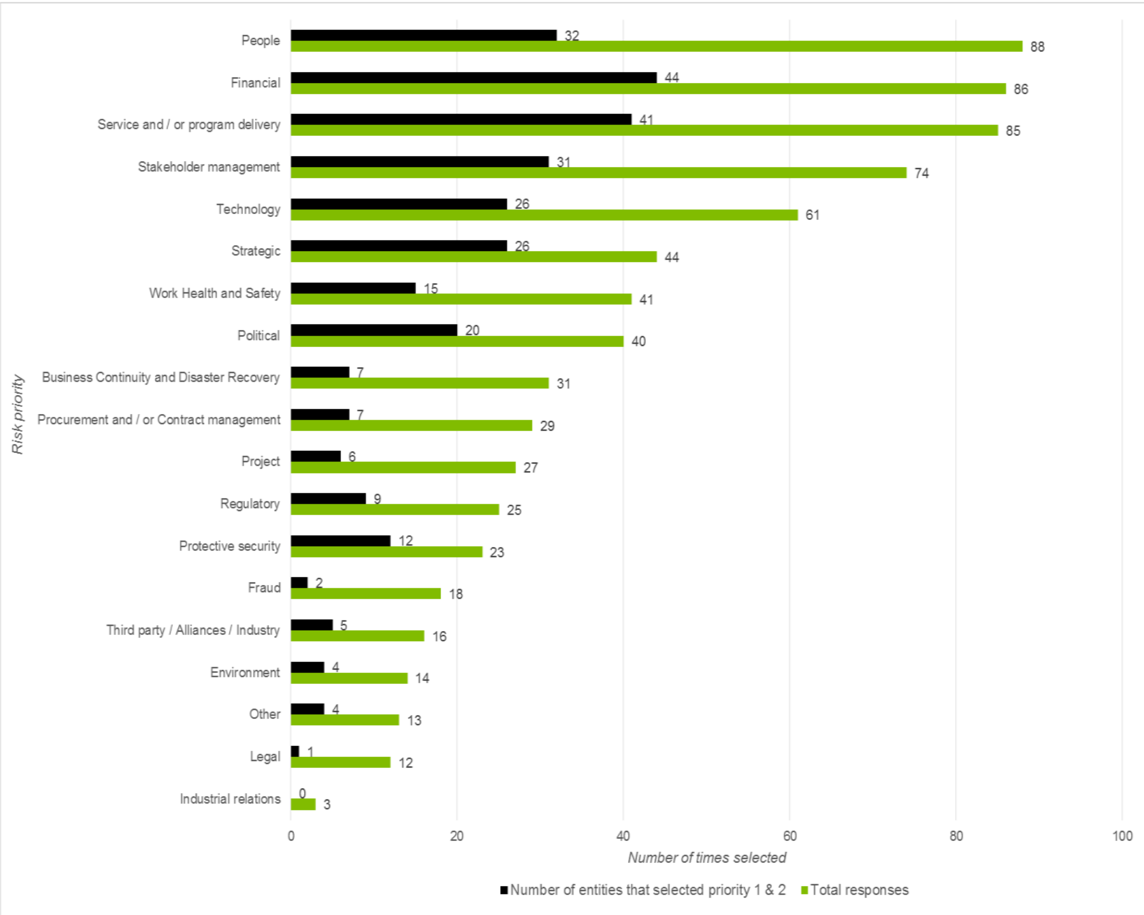
The shift in top emerging risk priorities was most pronounced in the movement of Political sources of risk out of the top four this year, from second most important in 2016, with Technology increasing in significance for many entities as a future source of risk.

Financial and Service and / or program delivery remain sources of risk most relevant for the Fund both currently and into the foreseeable future, as was seen in 2016. Financial risk stands out as a clear leader in risk priorities - even more so in 2017 than 2016 with a 15% increase compared with last year's results.

Graphs 5A and 5B illustrate both these highest priority risk sources and the total number of votes for a risk source at any of the five priority levels. This comparison introduces the sources of risk that, while not at the absolute forefront of the Fund's risk agenda, are still afforded considerable attention and are perhaps more relevant to particular types of entities.

Graph 5A shows that, while just over 20% of entities prioritised People as either their first or second current risk priority, the vast majority of entities (approximately 90) included this source of risk as one of their top five. Similarly, for Financial, Service and / or program delivery and Stakeholder management as sources of risk, the vast majority of the Fund prioritised these as one of their top five priorities.

Graph 5A: Current risk priorities ranked by total responses



Similar to results shown in Graph 5A, the results depicted in Graph 5B indicate that, while a smaller proportion of entities selected Technology, People and Stakeholder management as their top emerging risk priority, the majority of the Fund ranked these somewhere in their top five priority areas on the horizon.

Graph 5B: Emerging risk priorities ranked by total responses