Chapter 6

Compliance and awareness

6.1 Based on its examination of Defence's acquisition process the committee found that on paper at least Defence has a robust risk management regime, which is comprehensive, systematic and engages all stakeholders. Further, that if followed correctly, risk would be considered from the outset or formative phase of a project when critical decisions are made and then managed throughout the project including a continuous process of identifying, analysing and mitigating risk. Defence's key policy documents explicitly recognise risk management as an essential part of corporate governance and senior Defence leaders have stated their commitment to sound risk management practices.

6.2 In this chapter, the committee examines the implementation of Defence's risk management strategies. It compares Defence's stated policy on risk management and the advice contained in its relevant guides on procurement with practice and actions. Having determined that Defence's policy and advice on risk management is not the problem, the committee's purpose in drawing these connections is to better locate the source of poor decision-making and performance.

Problems in defence procurement

6.3 Evidence before the committee identified significant failings in a number of major projects. They included inadequate description of risk during capability definition and planning phase; underestimation of the maturity of the technology and/or complexity of integration; and miscalculation of industry's capacity to deliver. In essence, a failure to understand, appreciate and mitigate risk. Indeed, Defence in its submission recognised that the common causes of poor project performance noted from past and current projects of concern are:

- unachievable expectations in terms of technology, performance or schedule;
- scope changes;
- ineffective defence stakeholder engagement and interaction; and
- challenging commercial or business relations.

6.4 In this context, the committee believes that it is important to refer again to the finding of the Helmsman Institute that some of the complexity in Defence's acquisition projects was 'self-inflicted'. It cited factors such as embarking on highly developmental projects; level of customisation; limited clarity on the key drivers of the project; lack of clear plans to achieve target dates and results; and tension between the needs of the military chain of command and the requirement to deliver against defined contracts and commitments.[1] The causes of poor project performance identified by Defence and the Institute's observation about 'self-inflicted' complexity indicate that although Defence has a solid risk management policy, in practice it is not working to full effect.

Culture of risk management

6.5 Having examined risk management in the UK MoD, Mr Chris Maughan, defence analyst, was compelled to ask that if the MoD had the right process, guidance documentation and tools why then was risk management not delivering the anticipated benefits. In his opinion 'the answer can only lie in its actual implementation'.[2] He found:

> For improvements to be experienced there needs to be a major shift, by the MoD, away from process and towards a concentration on comprehensive quantitative schedule and cost risk analysis. There needs to be an appreciation, within both MoD and the wider defence industry, of the root causes of the failure of risk management and a willingness to take the necessary actions to resolve them.[3]

6.6 This observation has direct relevance for Australia's Defence organisation. Indeed, a number of the independent members of the gate reviews cited risk identification, mitigation and management as one of the major challenges for Defence and an area in need of 'significant attention'.[4] Dr Ralph Neumann stated:

> It is not a matter of process: the process exists. It is a matter of better understanding the business, focusing on things that matter and better utilising the opportunities to reduce risk rather than managing the fallout of the risks.[5]

6.7 In the previous chapter, the committee noted that to be effective a risk management regime should be:

> …fully integrated and embedded in an organisation's culture so that risk management policy and practice is part of management thinking and actions and permeates all levels of the organisation—enterprise level, function level

[1] The Helmsman Institute, *A Comparison of Project Complexity between Defence and other Sectors*, public release version, p. [11–13].

[2] Chris Maughan, 'Risk Management in Defence Procurement', RUSI Defence Systems, June 2010, p. 95. A former Royal Navy officer, Chris Maughan is a Managing Consultant with Decision Analysis Services Ltd, and since 1989 has been responsible as project manager for the delivery of risk, project management and technical due diligence support to a number of major programs for clients worldwide.

[3] Chris Maughan, 'Risk Management in Defence Procurement', RUSI Defence Systems, June 2010, p. 96.

[4] Dr Neumann, *Committee Hansard*, 13 June 2012, p. 3.

[5] *Committee Hansard*, 13 June 2012, p. 3.

> or business unit level—senior managers in particular must show leadership and commitment and managers at all levels must take responsibility.[6]

6.8 Despite the clear statement of commitment to risk management, evidence presented to the committee suggests that risk management may not be front and centre of people's thinking in defence procurement. The first indication is the extent to which personnel adhere to the guidance or directions issued in Defence's handbooks and instructions.

Adherence to procurement policy and guidelines

6.9 Compliance is essential if Defence's risk management policies and their supporting guidelines and manuals are to translate into organisation-wide practice. In its preliminary report, the committee noted problems caused by non-compliance with such directions and advice. For example, the Defence Teaming Centre described the Defence Procurement Policy Manual as 'robust', but noted that 'it is the differential tailoring and interpretation of these policies by the DMO that causes significant frustration and confusion for industry'.[7] It suggested that training in the interpretation of the manual across DMO would create 'a consistent interpretation and implementation' of the Manual.[8] This practice would encourage a 'more fluid and efficient procurement process with both the customer and contractor understanding and having the same interpretation of the policy'.[9]

6.10 Likewise, the Australian Industry Defence Network agreed that DMO's procurement procedures and processes as detailed in the procurement manual appear sound. It noted, however, that the poor implementation and apparent non-compliance with the DCP, Defence Procurement Policy Manual and the Defence Capability Manual schedules and processes adversely affected the acquisition and sustainment of ADF capability on a regular basis.[10] In this regard, the committee notes ANAO's audit report on Planning and Approval of Defence Major Capital Equipment Projects, which examined the key capability development documents from a sample of 20 Defence projects. The ANAO found that Defence was not consistently adhering to its 'administrative framework for implementing the process'.[11]

[6] See for example, Ian McPhee, Deputy Auditor-General for Australia, 'Risk Management and Governance', Speech, National Institute for Governance, Canberra, 16 October 2002, p. 2; Department of Defence, Defence Science and Technology Organisation, Svetoslav Gaidow and Seng Boey, *Australian Defence Risk Management Framework: A Comparative Study*, Commonwealth of Australia, 2005; and Standards Australia, *Delivering assurance based in ISO 31000:2009 Risk Management—Principles and guidelines*, HB 158–2010, paragraph 1.2.

[7] *Submission 16*, p. 1.

[8] *Submission 16*, p. 2.

[9] *Submission 16*, p. 2.

[10] *Submission 19*, p. 3.

[11] ANAO Audit Report No. 48 2008–09, *Planning and Approval of Defence Major Capital Equipment Projects*, 2009, paragraph 11.

6.11 Along the same lines, the Pappas Report observed that the manner in which projects approach the management of risk was somewhat variable. According to Mr Pappas, the quality of detail on the type/level of risk, residual risk post-treatment, and ownership of risk was also inconsistent. He noted that a risk register had been in place for some post-Kinnaird projects, but there was no standardised template. According to the Project Management Manual, a project risk log should be established in the Needs Phase and is mandatory for second pass.[12] The log should be used 'to record all project risks, the likelihood, consequence and level assigned to each, the treatment strategies (if the risk is unacceptable), the amount of Project Contingency Budget assigned to each treatment and the individual responsible for managing risk'.[13] The integrated project team is to review the risk register and treatment strategies, at least monthly.[14]

6.12 Despite the existence of a risk register, Pappas found that 'some mitigation strategies had not been implemented and lacked a rationale or timeline indicating when the action was to be implemented and the success of the mitigation reviewed'. He recommended that technical risks should be measured and managed through a risk register with a standard format and clear action plans.[15]

6.13 In its performance audit into acceptance into Service of Navy capability, the ANAO observed that mis-matched expectations between DMO and Navy had adversely affected the acceptance into service process. It identified a range of factors that could result in misunderstandings or disagreements including instances of projects proceeding with high-level risk because of a lack of agreed Capability Definition Documents and Certification Plans and Systems Safety Plans.[16] The audit report found:

> …without the application of greater discipline by defence in the implementation of its own policies and procedures, improved communication and collaboration across the relevant parts of the defence organisation during a project's life cycle and the maintenance of adequate records to support appropriate monitoring of capability development performance, the necessary improvements in acquisition outcomes will not be achieved.[17]

[12] Department of Defence/Defence Materiel Organisation, *DMO Project Management Manual, (PMM) 2009*, 10 August 2009, paragraph 7.11.

[13] Department of Defence/Defence Materiel Organisation, *DMO Project Management Manual, (PMM) 2009*, 10 August 2009, paragraph 7.11.

[14] Department of Defence, *Defence Capability Development Handbook,* August 2011, paragraph 3.2.16.

[15] *2008 Audit of the Defence Budget*, Commonwealth of Australia, 3 April 2009 (Pappas Report), pp. 82–83.

[16] ANAO Audit Report No. 57 2010–11, *Acceptance into Service of Navy Capability*, 2011, paragraph 7.60.

[17] *Committee Hansard*, 11 August 2011, p. 24.

6.14 Finally, the committee draws attention to the ANAO's observations in the annual Major Projects Reviews where it continues to report on a lack of consistency in the application of policies, practices and systems relevant to risk management. In the most recent reviews, it noted that the different practices at a project level 'impact on a consistent and strategic risk management approach at the whole of the DMO level'.[18]

6.15 There could be a number of reasons for this non-compliance, inconsistency or laxity in applying guidelines including a lack of awareness, complacency, or no one person or group having responsibility or being accountable for their part in the process. Assumptions that someone else will check the veracity of the information before them or an absence of, or ineffective, oversight of the process may also contribute to the lack of regard shown toward the manuals and guidelines. A combination of both these cultural and structural factors may be at work that results in non-compliance. It may well be that the culture took root and flourished in Defence's environment of ill-defined organisational accountability.

Awareness and ownership of risk

6.16 A healthy risk management environment is one where all members of an organisation are fully aware of the risks, controls and tasks for which they are accountable.[19] For example, in 2002 the Deputy Director, ANAO, referred to the importance of having a clear view on what is an acceptable level of risk.[20] In this regard, Dr Thomson cited the project for 12 new submarines, suggesting that:

> You cannot pretend that risk away, you have to look at that risk and stare it in the face. It has to be part of your decision making but I do not think we should throw up our hands and give up on doing things. We should simply take an objective and sober recognition of the risks that some of these options carry because of the present state of our engineering and other expertise.[21]

6.17 DMO's Project Management Manual makes absolutely clear that there is 'ownership of risks and controls'.[22] Two of the key principles enunciated in the manual are:

- risks are not avoided, but rather managed at the level at which people have the authority, responsibility and resources to take action; and

[18] See for example, ANAO Report No. 17 2010–11, *2009–10 Major Projects Report*, paragraph 31 and ANAO Report No. 20 2011–12, *2010–2011 Major Projects Report*, paragraph 42.

[19] Standards Australia/Standards New Zealand, *Risk Management—Principles and guidelines*, AS/NZS ISO 31000:2009.

[20] For example see Ian McPhee, Deputy Auditor-General for Australia, 'Risk Management and Governance', Speech, National Institute for Governance, Canberra, 16 October 2002, p. 20.

[21] *Committee Hansard*, 12 August 2011, p. 15.

[22] Department of Defence, *DMO Project Management Manual DMM (PMM) 2009, Interim,* August 2009, paragraph 7.3.

- a risk management culture is promoted and is part of everyone's job.[23]

6.18 In their recent audit of acceptance into service of Navy capability, the ANAO found some significant issues with Navy projects including 'that Navy, CDG and DMO did not have a shared understanding of the risks to the generation of the expected capability from Navy projects and had not taken shared responsibility for mitigating those risks'.[24] The Pappas Review also suggested that a 'clearer indication of the most critical risks would help those tasked with risk management to know where to focus'. Worryingly, it observed that DSTO's involvement and assessments of project options were 'not always paid the respect they should be'.[25] It should be noted that DSTO has a central role in providing technical risk assessments especially for first and second pass approval.

6.19 This devaluing of advice from technical experts by non-experts points to an organisational weakness. Furthermore, as noted in chapter 2, DSTO is not the only body of technical experts whose advice may be neglected. Within Defence the advice of domain experts and operators does not always inform key decisions, sometimes with unfortunate results. There appears to be no effective mechanism to ensure that critical technical advice is accurately reflected in submissions on major acquisitions to senior decision-makers and ultimately to government—no real contestability; no visibility of risk.

6.20 In respect of risk awareness, Mr King expressed concern that some people in Defence do not fully appreciate the critical importance of risk analysis, monitoring and management. He stated:

> There is a problem we need to deal with in defence more rigorously than we sometimes do: we become a bit unreactive to red alarms. In other words, we see a risk and we watch it go through to fruition and say, 'Oh, yes, indeed it did happen'. That is happening less and less where we are focusing on what is a risk and what we are doing about it. Unfortunately, sometimes that materialises in a project of concern, when we have to go and do a new remediation project to get it right.[26]

6.21 Mr King stated that he tells his personnel that there are really only two sins they could commit—not knowing their risks or problems, and not telling anybody about it or not doing something about it. He explained that DMO is trying to encourage its people, when they have this risk**,** just not to talk about how they are 'monitoring it' or 'actively checking it', but to have a real plan to mitigate or treat it. According to him, more often than he would like, Defence have had a risk that it has

[23] Department of Defence, *DMO Project Management Manual DMM (PMM) 2009, Interim,* August 2009, paragraph 7.5.

[24] *Committee Hansard*, 11 August 2011, p. 24.

[25] Department of Defence, *2008 Audit of the Defence Budget*, 3 April 2009, pp. 3 and 82.

[26] *Committee Hansard*, 7 October 2011, pp. 25–26.

'allowed to come to fruition without a real remediation plan'. He told the committee that 'we need to work harder at that'.[27]

6.22 The Rizzo Report observed that Defence was beginning to develop mechanisms to quantify its appetite for risk 'in a formal way and to promote this vertically through the organisation'. It noted, however, that this practice 'needs to become part of everyday life in Defence, with effective risk management being adopted and linked throughout'.[28]

Committee view

6.23 Despite Defence's clear commitment to sound risk management and to the principle of promoting a risk management culture which is seen as 'part of everyone's job', some personnel fail to own risk and avoid rather than manage it. Indeed, evidence before the committee presents a compelling case that Defence must take risk management more seriously. Mr Pappas' description of the 'variable' approach to recording risk management activities is consistent with Mr King's comments about some personnel being unresponsive to emerging risks.

6.24 The fact that some defence personnel appear inattentive to, or unmindful of, risk or uncertain about their role in risk management must be symptomatic of a deeper systemic problem in defence procurement. This failure to own risk is not a process problem—it is clearly an organisational weakness that effectively permits people to avoid taking responsibility.

Learning lessons and recordkeeping

6.25 As noted in the previous chapter, to be effective, risk management should be part of a continuous improvement system where experiences in risk inform revised risk assessment and management strategies. This means that lessons must be learnt from previous experience and applied to future decisions and actions regarding risk management.[29] As Air Marshal Binskin, Vice Chief of the Defence Force, told the committee:

> It is only a lesson learnt if you do not repeat it: otherwise it is just a lesson identified and it is useless.[30]

6.26 Industry representatives were of the view, however, that:

[27] *Committee Hansard*, 7 October 2011, p. 26.

[28] Department of Defence, *Plan to Reform Support Ship Repair and Management Practices*, July 2011, p. 10. Mr Rizzo recognised that risk management should be 'a central function in Defence'.

[29] See for example, Tzvi Raz and David Hillson 'A Comparative Review of Risk Management Standards', *Risk Management: An International Journal 2005*, vol. 7, no. 4.

[30] *Committee Hansard*, 5 October 2011, p. 56.

> At the moment Defence is not capable of being able to capture lessons learnt and project those lessons learnt forward a decade. What tends to happen is that they end up repeating a number of mistakes which lead to relearning of those lessons.[31]

6.27 For example, the Defence Teaming Centre stated that the DMO 'appears to lack any capacity to learn from failings in previous projects'. It suggested that there does 'not appear to be any drive or motivation within the DMO to capture lessons learned and pass them on internally and to industry'.[32] The pattern of repeated shortcomings in projects as detailed in chapter 2 attests to Defence's difficulties in learning from past mistakes.

6.28 In its guide to risk management, Standards Australia suggests that the 'results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the risk management framework'.[33] It stated further that risk management activities should be traceable.

6.29 In some cases, however, it was not the absence of records that was the problem but the quality of the documentation, which reflected a poor understanding of what was important and what was not. Many witnesses referred to Defence's procurement of major capital equipment as process bound. One referred to people in Defence getting 'bogged down' with too much paper work.[34] A number of independent members of the gate review boards observed that although improving, the standard of documentation could be lifted.[35] One noted 'a certain amount of nugatory work…and at times a lack of guidance of project direction that can occur pre project approval'. In Dr William's view there was 'an issue of quality and consistency'. He noted:

> On some occasions I think there is an enormous amount of work put in to produce extremely large documents which are probably far more so than is needed—and it is done with the best will in the world but it must tie up a lot of resources. I think perhaps in some cases if we could not actually remove documents we could at least streamline them, and that would be quite a resource saver.[36]

6.30 Mr Gallacher was similarly aware of instances where the project team were 'spending enormous amounts of effort on doing detailed work but then missing

[31] *Committee Hansard*, in camera.

[32] *Submission 16*, p. 2.

[33] Standards Australia/Standards New Zealand, *Risk Management—Principles and guidelines*, AS/NZS ISO 31000:2009, paragraph 5.6.

[34] *Committee Hansard*, 12 June 2012, p. 35.

[35] Dr Neumann, and Mr Irving, *Committee Hansard*, 13 June 2012, pp. 16–17.

[36] *Committee Hansard*, 13 June 2012, p. 17.

important things that were going on'. He supported 'simplifying rather than adding complexity'.[37]

6.31 In the risk management process, records provide the basis for improving methods and tools, as well as the overall process.[38] The committee has commented on the haphazard use of the risk register—an important accountability and learning tool—which not only highlights Defence's poor record keeping but points to a deeper problem with risk management in the organisation. The observations about the inability of personnel to discern the important issues from the less important when producing documentation similarly suggests that other factors are at work when it comes to effective risk management. For example, evidence presented later in this report suggests that even though people are diligent and hard working they may feel disempowered or unable to effect change, may be the wrong person to make decisions about risk, or may not have the requisite qualifications and experience to recognise the significance of risks.

Conclusion

6.32 In order to identify deficiencies in the acquisition process, the committee considered the practical application of Defence's risk management practices and procedures as set down in its written guidelines and manuals. The committee found that, if followed correctly, the acquisition process should ensure that risks are identified early and managed appropriately. Clearly, however, in some cases problems emerge or are exacerbated in an acquisition project because of poor implementation of Defence's policy and guidelines. The committee finds statements indicating that defence personnel are not alert to risk most disturbing. There can be no excuse for such personnel disregarding their own procedures, which can result in the organisation being unaware of, downplaying or ignoring, risks that threaten the success of a major acquisition. In effect, as stated by Mr King, Defence must not allow situations to develop where personnel watch risk emerge and come to fruition without a remediation plan. Poor recordkeeping and inappropriate or incomplete documentation is yet another indicator of a poor risk management regime. In essence, despite Defence's risk management policies and guidelines, the evidence is clear and unequivocal that in practice Defence's risk management in a number of major defence acquisition projects has:

- failed to identify risk during the early stages of an acquisition project or, as highlighted in chapter 2, if identified, especially by domain experts, risk was downplayed, misinterpreted, or ignored;
- failed to monitor risk and its treatment on a systematic basis throughout the procurement process; and

[37] *Committee Hansard*, 13 June 2012, p. 17.

[38] Standards Australia/Standards New Zealand, *Risk Management—Principles and guidelines*, AS/NZS ISO 31000:2009, paragraph 5.7.

- failed to ensure that senior leaders and government were fully apprised of the nature and extent of risk resident in a project.

6.33 The question must then be asked—who is responsible and accountable for risk management: for ensuring that 'things do not go wrong', or if they do, for prompt remedial action. In the following chapters, the committee continues to seek to understand the reasons for poor performance when it comes to identifying and/or acting on potential problems. It considers accountability and responsibility; communication and reporting within the organisation.