The Auditor-General
Audit Report No.19 2011–12
Performance Audit

Oversight and Management of Defence's Information and Communication Technology

Department of Defence

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81224 1

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

Or via email:
webmaster@anao.gov.au

Australian National
Audit Office

Canberra ACT
20 December 2011

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Department of Defence in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit, and the accompanying brochure, to the Parliament. The report is titled *Oversight and Management of Defence's Information and Communication Technology*.

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

Yours sincerely

Ian McPhee
Auditor-General

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

AUDITING FOR AUSTRALIA

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

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone: **(02) 6203 7505**
Fax: **(02) 6203 7519**
Email: **webmaster@anao.gov.au**

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team
Ramon Marquardt
Peta Martyn
Kim Bond
Fran Holbert

Contents

Abbreviations 7
Glossary 9

Summary and Recommendations 11

Summary 13
Introduction 13
Audit objective and scope 15
Overall conclusion 16
Key findings by Chapter 21
Agency response 28
Recommendations 29

Audit Findings 31

1. Introduction 33
Defence Information and Communication Technology 33
Improving ICT services in Defence 37
Integrating Defence's strategic imperatives for ICT reform 45
Audit approach 47
2. Governance structures and decision-making processes 49
Introduction 49
Governance structures for Defence's ICT 50
Strategic ICT management 56
Defence ICT approval framework arrangements 65
Assessing ICT proposals 73
3. ICT investment, benefits and risks 75
Introduction 75
Financial investment in ICT 78
Benefits planning and management 82
Risk management 86
4. Chief Information Officer Group management maturity 94
Introduction 94
CIOG as a program manager for Defence 97
P3M3® process perspective maturity assessments 100
The need for improved portfolio and program management maturity 123

Appendices 129

Appendix 1: Reviews of Defence ICT 131
Appendix 2: Major ICT Initiatives 133
Appendix 3: P3M3® Maturity Levels 137
Appendix 4: Strategic Reform Program Streams 141
Index 142

Series Titles 144
Current Better Practice Guides 147

Tables

Table 1.1 SRP stream ICT initiatives 41
Table 1.2 Defence ICT strategic guidance documents 45
Table 2.1 Development of Defence's ICT Integrated Plan of Work 62
Table 2.2 Defence ICT initiative approval authority for capability development projects 68
Table 2.3 Recorded DICTC outcomes for 16 ICT proposals considered from July 2008 to October 2010 71
Table 3.1 Key indicators tracking the SRP ICT stream performance 84
Table 3.2 January to June 2011 SRP ICT stream performance report 85
Table 3.3 SRP initiatives with ICT involvement 89
Table 4.1 Development pathway for portfolio and program management 97
Table 4.2 Analysis of critical ICT dependencies in the SRP 105
Table 4.3 2009 proposed plan to address the resource shortfall 120
Table A 1 Major ICT Initiatives 133
Table A 2 P3M3® Maturity Levels 137
Table A 3 Strategic Reform Program Streams 141

Figures

Figure 1.1 The common, shared and unique layers of the Defence Information Environment 36
Figure 1.2 DICT Strategy: strategic imperatives, elements and initiatives 44
Figure 1.3 Delivering on Defence ICT strategic imperatives: integrated ICT reform program 46
Figure 2.1 Defence Senior Management Committees and ICT governance and decision-making structure, October 2011 51
Figure 2.2 Defence's estimated ICT expenditure, 2010–11 58
Figure 2.3 Defence's planned ICT initiatives approval framework 66
Figure 2.4 The Defence ICT investment two-pass approval process and gateway 72
Figure 4.1 P3M3® structure 95
Figure 4.2 Overview of CIOG functions 101
Figure 4.3 CIOG management structure 102

Abbreviations

ADF	Australian Defence Force
CDF	Chief of the Defence Force
CIO	Chief Information Officer
CIOG	Chief Information Officer Group
DARC	Defence Audit and Risk Committee
DBA	Defence Budget Audit
DC	Defence Committee
DCP	Defence Capability Plan
DICTC	Defence Information and Communication Technology Committee
DICT Strategy	Defence Information and Communication Technology Strategy
DIE	Defence Information Environment
DIEC	Defence Information Environment Committee
DMO	Defence Materiel Organisation
DRN	Defence Restricted Network
DSN	Defence Secret Network
DSSRG	Deputy Secretary Strategic Reform and Governance
DSTO	Defence Science and Technology Organisation
FIE	Fleet Information Environment
I&S	Defence Intelligence and Security Group

ICT	Information and Communication Technology
IPW	Integrated Plan of Work
KPIs	Key Performance Indicators
PDM	Defence ICT Program Design Manual
PMO	Portfolio Management Office
SET(s)	Stakeholder Engagement Team(s)
SRGE	Strategic Reform Governance Executive
SRP	Strategic Reform Program
WFMC	Workforce and Financial Management Committee

Glossary

Information and Communication Technology (ICT)	ICT encompasses all hardware, software, personnel and services involved in the design, development, implementation, maintenance, support, sustainment, operation and management of technologies to store, retrieve, manipulate and communicate computer based information. This includes software applications, computer hardware and support services to convert, store, protect, process, transmit, and securely retrieve information.
Defence Information Environment (DIE)	The DIE comprises the information used by Defence and the means by which it is created, managed, manipulated, stored, disseminated and protected. The DIE's two main elements are information domains and information infrastructure, and it encompasses all assets and capabilities involved in the exchange of information by computers and communications across all security domains used by Defence for military operations and Defence business.
Network	A computer network is a collection of computers and devices interconnected by communication channels that facilitate communication among users, and allow users to share resources.

Summary and Recommendations

Summary

Introduction

1. Information and communication technology (ICT) supports the war fighting and intelligence capabilities of the Australian Defence Force (ADF), and Defence's corporate functions.[1] The Defence Information Environment (DIE) is one of the largest ICT networks in Australia. At an estimated annual cost of $1.2 billion in 2010–11, the DIE connects over 500 Defence sites within Australia and overseas.[2] The network provides services ranging from highly diverse and complex weapons support systems and electronic counter-insurgency, to more straightforward day-to-day services such as word processing. The effective and efficient management of this extensive ICT network is a major challenge for Defence and is critical to the achievement of its strategic objectives.

2. Historically, Defence's ICT infrastructure and application services have been defined and acquired in support of individual initiatives and capability needs. Accordingly, Defence's ICT has tended to grow and operate in a fragmented way, resulting in gaps in service delivery, duplication, redundancy, and impaired inter-operability. Consequently, the performance and reliability of Defence's ICT has been adversely affected, and support and maintenance has been difficult and costly. Defence recognised these issues and, in 2009, the then Minister for Defence articulated the need for ICT reform, noting that it would take time to achieve the desired level of ICT service capacity:

> Defence faces real problems with its own infrastructure. Some of Defence's ICT systems are antiquated and inadequate for Defence's complex operational requirements as a result of being grossly under-funded for years. Some of the

[1] Defence comprises the Australian Defence Force (ADF), the Department of Defence, and the Defence Materiel Organisation (DMO). The Defence Groups are the functional areas that deliver Defence outcomes and/or support those that do. The ADF is made up of the three Services: Navy, Army and Air Force.

[2] Department of Defence, Chief Information Officer Group, *Defence Information Infrastructure (DII) Plan – Financial Year 2007–2008*, p. 19.

department's ICT systems are now too cumbersome, fragile, and costly to operate effectively.[3]

3. The Minister's concerns, especially the pressing need for Defence to improve its ICT management, were also expressed in the findings of management reviews of Defence over the period 2007 to 2009.[4] In particular, the 2007 Defence Management Review set out an ICT reform agenda, recommending that Defence appoint a Chief Information Officer (CIO, appointed in 2007) and develop an enterprise-wide ICT strategy. In November 2009, Defence released an *Information and Communication Technology Strategy* (the DICT Strategy), which articulated Defence's plan to address the shortcomings in its ICT governance, planning and control frameworks.

4. The DICT Strategy was developed during the same period as the Government's May 2009 Defence White Paper (the White Paper) and the 2009 Strategic Reform Program (SRP). The White Paper and the SRP propose ICT reform in support of war fighting and business reform objectives for Defence through to 2030.[5] Over the decade to 2019, the SRP is intended to provide $20 billion in savings for re-investment in the Defence capabilities set out in the White Paper.[6] ICT reforms alone are required to contribute $1.9 billion towards the overall SRP savings target, and the success of over half of the SRP reform streams[7] is critically dependent on the provision of effective ICT services,

---

3 The Hon John Faulkner MP, Minister for Defence, speech to the Australia and New Zealand School of Government, *Governance and Defence, Some Early Impressions*, 13 August 2009.

4 These include: *Defence Management Review; Defence Budget Audit; CIO review of ICT;* and the *Defence White Paper – Information and Communications Technology Companion Review*.

5 See Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030,* 2009, p. 115 and Department of Defence, *The Strategic Reform Program 2009: Delivering Force 2030,* 2009, p. 21.

6 In the 2009–10 Budget, the Government set Defence a fixed funding model to provide additional funding of $146 billion to fully fund the White Paper over 21 years to 2029–30. Under the model, Budget funding to Defence will have 3 per cent average real growth to 2017–18, 2.2 per cent average real growth from 2018–19 to 2029–30 and 2.5 per cent fixed price indexation from 2009–10 to 2029–30, with the 2.5 per cent to be calculated from 2009–10 but applied only from 2013–14. Under these arrangements, the $20 billion gross savings from the SRP and other initiatives will accumulate in the Defence Strategic Investment Reserve for re-investment in higher priority Defence capabilities. Fixed funding applies to all years individually over the 21 year period and cannot be exceeded in any individual year. Defence will continue to seek supplementation for operations on a no-win, no-loss basis. See Department of Defence, *Budget portfolio Statements 2009–10*, May 2009, p. 15, and Department of Defence, *Incoming Government Brief,* Circa 2010, p.6-1, from <http://www.defence.gov.au/foi/docs/disclosures/101_1011_igb.pdf> [Accessed 24 October 2011].

7 The Strategic Reform Program comprises 15 separate reform streams. Seven of the streams are designed to deliver $20 billion in savings to Defence, while eight streams are non-savings streams. The eight streams dependent on two or more ICT projects consist of five savings streams and three non-savings streams. The 15 reform streams are set out in Appendix 4.

including infrastructure, applications development and sourcing. Significant aspects of the SRP require ICT-enabled business transformation, with the attendant potential benefits and risks:

> A fundamental principle [*behind increased investment in ICT*] is that it will deliver better cost effectiveness through the streamlining and amalgamation of corporate support activities…The financial risks associated with IT-enabled business change are due therefore not only to the scale of the programmes and projects themselves, but to the benefits they need to achieve and the pressure to produce return on investment.[8]

5. Defence's ICT reform program and the SRP foreshadow significant change in the administration of Defence, during a time of substantial ongoing involvement in operations. In addition, Defence is currently moving to implement the recommendations of the *Review of the Defence Accountability Framework* (the Black Review[9]), including presenting quarterly reporting against performance benchmarks set out in an Annual Defence Plan.

6. Defence informed Parliament in October 2011 that it anticipated adjusting the SRP and the implementation of the White Paper in the light of the outcomes of current internal reviews of the Defence budget, the capability development process, and the major projects in the 10-year Defence Capability Plan. The outcomes of these internal reviews will inform the formulation of the Defence budget in 2012–13.[10]

Audit objective and scope

7. The objective of the audit was to assess the development of Defence's oversight and management of its portfolio of ICT investments and projects. In particular, the audit examined Defence's:

- governance, strategic processes and decision-making structures that set out, prioritise and coordinate the integrated ICT reform portfolio and programs;

---

8 United Kingdom National Audit Office, 2006, *Delivering successful IT-enabled business change,* 2006, p. 24.

9 Black, R., *Review of the Defence Accountability Framework*, August 2011.

10 Senate, Foreign Affairs, Defence and Trade Committee, Additional Estimates Hearings, 19 October 2011, page 7.

- ICT risk management and capacity to identify and plan to achieve the benefits of its SRP ICT stream reforms (including methodologies to measure the realisation of savings and non-savings benefits);
- level of portfolio and program management maturity; and
- the impact of improvement efforts on Defence's ability to deliver the ICT services capacity required to support the SRP.

8. The ANAO's focus was on remediated or new Defence ICT capability resulting from the ICT reform program. Project management of individual ICT projects was not included in the audit scope.

Overall conclusion

9. Defence has commenced the vital work of remediating the publicly acknowledged deficiencies in its information and communication technology (ICT) systems. ICT reform is currently a major organisational agenda that is also expected to contribute substantially to the Strategic Reform Program (SRP). The SRP seeks to comprehensively reform Defence's business to support the policy, capability and funding expectations of the Government's May 2009 White Paper (the White Paper). Significant aspects of the SRP involve ICT-enabled business transformation. When the SRP was announced in May 2009, the Government announced that it would invest more than $940 million over four years to reform and remediate the Defence Information Environment (DIE) and its supporting infrastructure in order to support the White Paper objectives and achieve long-term ICT savings of $1.9 billion.[11]

10. Since then, Defence has made modest progress in improving the performance of its ICT systems and has started replacing obsolescent equipment. The SRP ICT stream exceeded its savings target in 2009–10 and met its savings target for 2010–11. At the time of this audit, the SRP ICT stream had reported total savings of $224 million (11.5 per cent of the stream target of $1.9 billion total savings over the period 2009–19) for expenditure of $249 million (26.5 per cent of total planned stream investment).

11. The Chief Information Officer Group (CIOG) has primary carriage of remediating Defence's ICT and the ICT initiatives and reforms supporting the

[11] The Minister for Defence, Hon. Joel Fitzgibbon MP, 2009, *Multi-million dollar investment to reform Defence ICT*, Media Release, Parliament House, Canberra, 2 May.

SRP. Since 2007, CIOG has sought to progressively map and cost all of Defence's ICT systems and investments, and develop a Defence-wide coordinated approach to ICT investment. In November 2009, CIOG set out an overarching Defence ICT Strategy to complement the White Paper. Along with the Deputy Secretary Intelligence and Security, the Chief Information Officer (CIO) is responsible for the governance of the SRP's ICT reform stream, thus achieving greater oversight of ICT planning and investment activity in Defence than in previous years.

12. At the time of its March 2010 progress report to the Government, Defence considered the SRP to be as complex an organisational reform agenda as had ever been undertaken in either the private or public sectors in Australia. Delivering ICT reform in Defence is a challenge of a very high order, entailing the simultaneous remediation of existing systems, the development of ICT systems critical to the SRP reform streams, and the achievement of savings at the upper bounds of feasibility. More than two years into the reform process, ICT continues to represent a material risk to the timely achievement of the SRP investment and savings targets set in support of the longer-term objectives of the White Paper.

13. To help manage these risks, Defence has taken steps to formalise and develop the governance and management of its ICT. Defence has established a high level governance committee—the Defence Information and Communication Technology Committee (DICTC)—to provide strategic direction for the planning, coordination and execution of ICT initiatives across Defence.[12] However, while the bulk of Defence's ICT investments to July 2013 will be in SRP related initiatives, DICTC is not well-integrated into the governance of the SRP. Decisions affecting the scope, timing, relative priority, and overall savings to be achieved by major ICT projects can presently be made by other high level Defence committees without the direct knowledge of, or coordination with, DICTC or CIOG. These other major committees include the SRP Stream Governance Committees, the Defence Workforce and Financial Management Committee, and the Defence Capability and Investment Committee. Coordination and information-sharing between these committees currently relies heavily on common membership, mainly of very high-level officials who are time-poor.

[12] The DICTC is supported by Intelligence, Military and Corporate sub-portfolio committees responsible for managing ICT priorities and requirements within their sphere.

14. While the impetus of ICT reform has started to erode Defence's compartmentalised management of its ICT, the absence of fully effective governance arrangements means that Defence ICT initiatives continue to be developed in the absence of processes to clearly identify and resolve competing priorities, properly identify interdependent initiatives, or provide a clear view of resources. Notwithstanding successive surveys of Defence's ICT environment, senior decision-makers are yet to have a reliable, consolidated view of Defence's ICT domain including all expenditure, servers and hardware, and software applications. CIOG's current knowledge of the Defence-wide ICT systems and expenditure, while the best available consolidation to date, is incomplete.

15. The multiple ICT reform agendas underway in Defence present particular complexity in the organisation's ICT portfolio. At the time of this audit, CIOG had direct visibility of some 75 per cent of Defence's ICT expenditure, which is a notable improvement on the situation at May 2009, when CIOG had visibility of less than half of Defence's ICT expenditure. Defence informed the ANAO that the improvement was due largely to:

> improved financial reporting of ICT, the Defence ICT Costing Baseline activity, which is now in its third year, and the ongoing maturing governance and consolidation of ICT infrastructure and software licences.

16. However, some $300 million of Defence's estimated $1.2 billion of ICT expenditure in 2010–11 was not directly visible to CIOG. While Defence's financial reporting of ICT has improved, the estimate of $300 million in expenditure includes information provided by Defence Groups and Service entities that is not necessarily compiled, recorded or calculated on a consistent basis. The lack of consistent Defence-wide ICT financial data has meant that, to estimate future expenditure and likely ICT savings, Defence has, in some cases, relied on data provided by consultants using proprietary estimation techniques that Defence is not in a position to verify or validate. Defence therefore has a less than complete view of the information needed to effectively manage its ICT, plan future systems, and fully deliver the savings necessary to support the White Paper targets.

17. It is also difficult for Defence to have a central view of all its ICT initiatives and proposals, as there are currently a range of different approaches and points of entry into its ICT approval processes. Without enterprise-wide processes for the development and approval of ICT initiatives, Defence is unlikely to be able to strategically guide its ICT reforms. CIOG has developed

a uniform set of approval processes, though they are yet to be fully implemented and applied to all initiatives. Defence informed ANAO in October 2011 that:

- in consultation with the Department of Finance and Deregulation (Finance), CIOG is currently finalising an ICT two-pass approval process to apply in Defence; and
- that the task of advising DICTC and the CIO of identified ICT interdependencies and conflicting priorities, including across the SRP reform streams, was now the responsibility of the Defence Information Environment Committee (DIEC).

18. These developments and activities are consistent with CIOG's November 2010 management maturity rating assessed under the P3M3® model mandated by the Australian Government.[13] The assessment indicated that, while ICT programs and projects were recognised as organisational investments, there were no standard portfolio processes, and limited consistency and coordination across programs and projects.[14]

19. As chief ICT service provider and de facto ICT program manager for much of Defence, CIOG's P3M3® management maturity ranking is in line with that of ICT management entities within other large Australian Government agencies. However, no other agency is currently undertaking such a large ICT-enabled business transformation as Defence's ICT reforms and the SRP, and CIOG's assessed level of management maturity presents risks arising from:

- the relative immaturity of standard portfolio-wide governance processes, such that they are not yet fully defined, documented, widely understood and consistently applied;
- the lack of a portfolio-wide view of ICT interdependencies and competing priorities;

[13] CIOG's November 2010 maturity ranking was given as 'Level 2 – Repeatable Process', which is set out in Appendix 3. CIOG's maturity rating is discussed in more detail in Chapter 4 of this report.

[14] The Portfolio, Programme and Project Management Maturity Model (P3M3®) provides a framework with which organisations can assess their current performance and put in place improvement plans with measurable outcomes based on industry best practice. Maturity ratings are given to seven organisational processes. The ratings range from one, which corresponds to management awareness that processes exist to bring goals into reality (though the processes may not be complete or may not be documented), through to higher levels of maturity up to a rating of five, at which processes are optimised.

- complex and sometimes confused accountability structures, including the absence of clear responsibilities for determining trade-offs among competing initiatives, and ambiguity in CIOG's role as coordinating capability manager for ICT; and
- a high level of demand on the CIOG's ICT capacity, currently some 350 staff short of projected requirements.

20. Defence is presently working to ameliorate these risks, which are acute. Most recently, Defence signed a contract with five preferred industry partners to improve ICT development, and alleviate immediate skills shortfalls and the pressure on Defence's own ICT resources.[15]

21. However, the risks remain high, as eight major SRP reform streams depend for their success on ICT projects, or on conjunct elements of ICT projects.[16] Schedule slippage is already evident and the failure or even the significant delay of one of these projects is likely to have a domino effect on other SRP activities that could delay or deny the anticipated flow of SRP savings into improved Defence capability. Defence's management of sustained high levels of ICT-related risk would benefit from program managers and SRP Streams adopting a full partnership model with CIOG to deliver these Defence portfolio initiatives. There is also a real need for CIOG to strengthen its organisational governance arrangements, to support the effective functioning of high-level governance bodies (including DICTC and the Strategic Reform Governance Executive–SRGE), and to clarify accountability.

22. Attaining a portfolio-level view of Defence's enterprise needs and managing it as a single entity is a challenging goal. In particular, the scale and complexity of Defence ICT requirements, the attendant organisational interdependencies, and the risks to the delivery of its transformation program underline the importance of the Defence leadership having a clear view of the strategic priorities for ICT. Inevitably, circumstances will change, requiring variations to plans. In this challenging environment, strong leadership focus will be required to deliver the benefits envisaged for the Defence organisation from the ICT transformation program over the next ten years.

---

[15] Announced 18 October 2011, at <http://news.defence.gov.au/2011/10/18/defence-selects-industry-partners/> [Accessed 19 October 2011].

[16] The eight major SRP reform streams are: Estate; Preparedness; Logistics; Smart Maintenance; Reserves; Army; Workforce and Shared Services; and Non-Equipment Procurement.

23. The ANAO made two recommendations aimed at clarifying the role of key elements of Defence's ICT management structure and improving Defence's portfolio-level oversight and management of its ICT.

Key findings by Chapter

Chapter 2 – Governance structures and decision-making processes

24. The effective planning and prioritisation of ICT projects is important to achieving an optimal balance between business-as-usual and ICT reform activities. To help align its ICT investments with the priorities set by the Secretary of Defence and Chief of the Defence Force (CDF), in 2008 Defence established the DICTC as its pre-eminent senior ICT committee. The role of the DICTC is to provide strategic direction for Defence's ICT investments through the review and prioritisation of all ICT initiatives and expenditure.

25. To assist DICTC, in 2008 CIOG provided the committee with information on the broad range of ICT activities and initiatives in Defence, which CIOG was in the process of mapping and costing. From its initial surveys, CIOG has subsequently developed a list of ICT projects, the current version of which is an Integrated Plan of Work (IPW) comprising 99 ICT projects, to assist DICTC and to articulate and guide Defence's ICT reform program.

26. Following the announcement of the SRP in May 2009, Defence separately established the joint ICT and Intelligence SRP Stream Governance Committee (the SRP ICT governance committee) which first met in June 2009. To help manage its ICT investments and facilitate stakeholder engagement in the SRP reform process, Defence established three SRP ICT sub-portfolio committees (the Military, Corporate and Intelligence sub-portfolio committees) and other Stakeholder Engagement Teams (SETs) to represent ICT business needs within the ICT reform process. The sub-portfolio committees and SETs have represented the Services' ICT priorities both to the DICTC and to the SRP ICT governance committee.

27. A key role of the SRP ICT governance committee is to help align Defence's ICT investments with SRP requirements. This role overlapped to an extent with that of the Defence Information Environment Committee (DIEC), established in August 2008 to advise the DICTC on the ICT planning cycle and, subsequently, on ICT-related matters associated with the SRP. DIEC is charged with providing advice on priorities within the IPW, coordinating stakeholder perspectives on ICT capability being considered by DICTC, and identifying

interdependent ICT projects and initiatives, including across the SRP reform streams. However, after being constituted in August 2008, DIEC became inactive until September 2010, and the SRP ICT governance committee did not meet between March 2010 and April 2011.

28. By early 2011, it was evident that the relationships between the Defence committees responsible for the governance of ICT reform, for the governance of the SRP ICT reform stream, and for the oversight of ICT initiatives supporting other SRP streams were not clear. By February 2011, Defence internal surveys of ICT stakeholders were reporting that ICT demand management and prioritisation were not functioning well, and that there was no effective decision-making for trade-offs between competing initiatives, including between the needs of stakeholder groups. For instance, though ICT initiatives underpinned other SRP reform streams, CIOG was not always included in stream governance arrangements and did not always have visibility of these ICT initiatives.

29. In addition, surveyed senior business stakeholders took the view that the business before DICTC was pitched more at immediate issues rather than at supporting strategic decision-making, providing DICTC with neither the lead-times nor the information suitable for informed strategic decision-making.[17] As a key support to DICTC, the CIO still has only limited visibility of the Defence-wide ICT costs and budget, and the ability of DICTC to formulate strategic direction for ICT within budget constraints was correspondingly limited.

30. After a hiatus of some months, during which the DIEC was effectively in abeyance and the SRP ICT governance committee did not meet, the relevant responsibilities of the two committees were clarified early in 2011. The SRP ICT governance committee met for the fourth time in April 2011. Defence informed ANAO in October 2011 that DIEC had not been effective in its intended role in respect of the SRP, which had instead been taken up by the SRP ICT governance committee.[18]

---

[17] Boston Consulting Group, *ICT Reform – Strategic Assurance Review*, February 2011, p. 6.

[18] Similar issues were canvassed in the 2011 Black Review, which noted that, 'Current accountability arrangements also constrain leadership capability and management capacity by reducing the ability of decision makers to exercise strategic control over the construction and implementation of decisions.' (see page 9). The Government accepted the findings of the Black Review and announced, among other things, a substantial reduction in the number of committees in Defence. Source: <http://www.defence.gov.au/oscdf/BlackReview/> [Accessed 24 October 2011].

31. Defence informed the ANAO in December 2011 of recent additional Shared Services and accountability reforms aimed at enhancing personal and institutional accountability, streamlining senior committees and the decision-making systems, and improving personnel skills development:

> The Shared Services review clarifies and strengthens the Coordinating Capability manager role of the CIO. Implementation of the Shared Services review outcomes, currently nearing completion of a ten week planning phase, will allow the CIO to have full visibility of the Defence-wide ICT systems and expenditure in a controlled and sustainable way.

32. Defence has also taken steps to clarify the approval processes for Defence ICT initiatives. At the time of this audit, three separate two-pass approval processes were in place:

- a Defence two-pass approval process coordinated by Capability Development Group, focused on capability acquisitions;
- the whole-of-government ICT two-pass approval process administered by the Department of Finance and Deregulation; and
- a CIOG-managed ICT Investment two-pass approval process.

33. There were multiple, uncoordinated entry points into Defence's ICT approval processes that were not well understood, giving rise to apparent inconsistencies in decision-making and the risk that Defence stakeholders would pursue individual, uncoordinated ICT solutions without the benefit of strategic guidance consistent with reforming Defence's ICT.

34. Defence informed ANAO in October 2011 that it was finalising the ICT two-pass process to apply in Defence, in consultation with the Department of Finance and Deregulation, and Defence stakeholders. The intention is to set out in detail the steps required, and CIOG has established a team to support and guide projects through the ICT two-pass approval process. This includes minor ICT projects, with some approvals already in train, though no project has completed the process to date. Defence informed the ANAO in December 2011 that:

> There are two approval processes for ICT projects: through the [Defence Capability Plan] or through …DICTC to the Whole-of-Government two-pass approval process. Minor projects from Groups and Services, go through an internal…process and then to the DICTC, having engaged with the relevant Stakeholder Engagement Team within CIOG.

> [*This*] is a reflection of the transition to a new approval process as we concurrently conduct a process trial that spans many months.

Chapter 3 – ICT investment, benefits and risks

35. An important element in reforming Defence's ICT was gaining a better understanding of the baseline information in respect of existing systems, particularly in terms of the extent and costs. At the time of the appointment of Defence's first CIO in 2007, Defence had only a limited overall view of its total ICT investments, including its annual expenditure on maintaining and improving its ICT infrastructure.

36. Since then, Defence has continued to refine its cost estimates, though it is yet to achieve full visibility of its ICT expenditure. Estimates provided by consultants in 2008 formed the basis of SRP ICT savings targets and indicated annual Defence ICT expenditure in the vicinity of $1.2 billion, excluding the cost of ICT components in deployable military equipment. Defence has undertaken additional work to develop ICT baseline expenditure estimates, and CIOG informed ANAO in October 2011 that its estimate for 2010–11 total ICT expenditure was $1.2 billion. Defence informed the ANAO in December 2011 that:

> The financial information populating the Defence ICT Costing Baseline has and continues to be progressively validated against the Defence financial systems (ROMAN and BORIS) records. This strategy is to ensure that Group and Service Heads understand and own the ICT activities that are performed within their own space.
>
> We have enough visibility of the Defence ICT spend to continue to deliver the ICT Reform Program. The implementation of Shared Services will progressively reduce the visibility gap in line with delivery of the ICT Reform Program. Significant progress has been made in this area.

37. The reform of ICT in Defence involves significant up-front investment in order to achieve long term savings and improvements in Defence's ICT support to its military and corporate functions. In particular, the SRP reforms set out an aggregate savings target for the SRP ICT reform stream of $1.9 billion to 2019, to be achieved from an investment of $940 million over the four years 2009–10 to 2013–14. However, Defence informed ANAO in October 2011 that it was unable to provide the underlying evidence supporting the derivation of the savings target, as it comprised estimates developed by external consultants using proprietary estimation techniques. In this circumstance, there is little evidence available to validate the processes used to

develop the SRP ICT savings target. While the work undertaken by Defence over the first two years of the SRP has given CIOG a much better understanding of Defence-wide ICT costs, it does not constitute a basis for validating the SRP ICT savings targets and investment schedule, or assessing the likelihood of the savings being realised.

38. Defence has developed Key Performance Indicators (KPIs) to measure the cash and non-cash benefits derived from the implementation of ICT projects. The non-cash KPIs provide an overview of the non-financial performance of Defence ICT reform activities, however only four of the total of 18 non-cash KPIs have established baselines, diluting their value to managers and decision-makers.[19] KPIs are more informative to decision-makers when they are prepared and reported with a frequency that supports the particular measure concerned, and Defence's non-cash KPIs relating to ICT would benefit from better-specified time-bound measures in order to provide information to decision-makers that is comparable over time.

39. Defence has in place a register of ICT project issues and risks, and accountability for attending to these is assigned at CIOG's weekly ICT reform meeting. However, the completeness of the CIOG ICT risk register, while improving over time, does not yet extend to all ICT risks, including those arising in other SRP reform streams. A key risk is that, while the majority of the SRP Reform Streams have some level of dependency on ICT capacity redevelopment, the mapping of SRP ICT interdependencies is still work in progress and is some way from completion. At present eight SRP streams are critically dependent on ICT initiatives, of which:

- seven streams are critically dependent on two or more ICT initiatives;
- most are heavily reliant on the early success of ICT initiatives for their long-term, overall success; and
- some are dependent on the same ICT initiative.

40. Ideally, the mapping of SRP ICT interdependencies would have received early attention. However, the first such mapping was only available within Defence from November 2010, and then only at a high level of

[19] The non-cash KPIs with established baselines were: reducing the number of data centres from approximately 200 to less than 10; increasing the proportion of ICT project expenditure from less than 10 per cent to more than 30 per cent of the expenditure on maintaining ICT business-as-usual; reducing the number of software applications on the DIE from some 3500 to less than 1000; and decreasing the number of ICT suppliers under contract from some 500 to less than 50.

generality. Mapping and managing ICT project interdependencies is important if Defence is to manage and deploy its ICT staff to greatest effect. Defence currently estimates its shortfall of core IT staff at 350 people, and the marked shortage of personnel to undertake the extensive ICT reform agenda ranks near the top of the risks cited for most Defence ICT initiatives.

41. Defence informed the ANAO that this is a challenging issue that is receiving significant senior management focus and, in October 2011, Defence entered into preferred partnership contracts with five key IT service providers. The partnership arrangements have the potential to afford Defence some flexibility in deploying its core IT staff and some resilience in the event of unexpected demands. However, building and retaining a core IT capacity to support Defence's sustained program of ICT reform remains a significant challenge and a continuing, significant risk.

Chapter 4 – Chief Information Officer Group management maturity

42. Management maturity models, notably the Portfolio, Programme and Project Management Maturity Model (P3M3®) of the UK Office of Government Commerce (OGC),[20] are now being widely applied to assess and help lift standards and capability in public sector management. In November 2010, CIOG received the results of a P3M3® assessment undertaken by an independent consultant.[21]

43. CIOG's assessed P3M3® maturity ranking of Level Two – Repeatable Process (briefly described at paragraph 18) was in line with those of equivalent ICT management entities within other large Australian Government agencies.[22] The key difference however, is that no other agency is currently undertaking such a large ICT-enabled business transformation as Defence's ICT reforms and the SRP.

44. Defence's shift from individual Services and Groups developing and managing their ICT, to a coordinated approach with CIOG as coordinating

[20] P3M3® is owned by OGC.

[21] Program Planning Professionals Pty Ltd (PCU3ED), *P3M3® Assessment Findings, Department of Defence – Chief Information Officer Group*, November 2010. The assessment responded to Finance's requirement that agencies subject to the *Financial Management and Accountability Act 1997* (FMA Act), including the Department of Defence, undergo a P3M3® assessment of their management of ICT. The assessment measured CIOG's capability to deliver its ICT investments and to plan capability improvements.

[22] The detailed descriptions of the P3M3® Maturity Levels are set out in Appendix 3.

capability manager for all Defence ICT is consistent with CIOG becoming Defence's ICT program manager within a larger portfolio. On this basis, the P3M3® assessment of CIOG is a reasonable guide to assessing the maturity of CIOG as a program manager with significant and diverse responsibilities for ICT within the Defence portfolio, including for ICT in the SRP investment portfolio.

45. The importance of improving the maturity of Defence's management of its ICT is accentuated by the scale of the ICT reform program and the underpinning and interdependent role improved ICT capacity will play in achieving the SRP objectives. Eight SRP streams (out of a total of 15) were found to have a critical dependency on CIOG ICT initiatives, creating a single-point-of-failure risk to more than half of the SRP streams. A high level of accurate and timely information on the progress of ICT initiatives is therefore essential to managing risk and realising benefits. However, while ICT is an essential enabler of major SRP Streams, CIOG has not always been incorporated as a full partner into those SRP Streams with heavy dependencies on ICT initiatives. A March 2011 internal Defence steering group found that:

> For the majority of projects, CIOG does not have visibility of when the SRP benefits are to be realised. Hence the desire to synchronise capability development and delivery with benefit realisation is a matter of luck rather than planning.[23]

46. Further, for the first time, Defence is operating with a fixed long-term funding model, setting the real rate of growth of funding to 2029–30.[24] Each year the Defence ICT budget will be reduced to achieve gross savings of $1.9 billion over the 10 years to 2019. This places additional pressure on CIOG to become more efficient and effectively manage its risks. Positively, the P3M3® assessment indicated that CIOG was on the path to providing effective management of Defence's ICT investment program, with some achievements to note and potential for more consistent application of management processes and improved coordination.

47. Defence's recent reviews of ICT reform in March and July 2011 noted that CIOG had successfully moved its focus from planning to executing ICT reforms. Defence informed the ANAO in December 2011 that it was making

[23] SRP Integration Steering Group, *ICT Support to SRP Streams*, March 2011.

[24] The long-term funding model is set out in footnote 6.

progress in partnering CIOG with SRP streams, notably in the human resource, finance and logistics domains, and hoped to extend the approach to other domains during 2011–12. However, further progress will also depend upon senior leadership support for corresponding improvements in the maturity of Defence's broader ICT governance and planning arrangements at the portfolio level. In particular, Defence would benefit from improved whole-of-enterprise ICT governance arrangements, including the setting of clear accountabilities across senior committees, improving the quality of management information (including ICT budgets and expenditure), and the active, high-level management of processes for resolving competing priorities and deciding trade-offs between ICT projects and stakeholders' ICT preferences.

Agency response

48. Defence responded to the report as follows:

> Defence acknowledges the findings contained in the audit report on the *Oversight and Management of Defence's Information and Communication Technology* and agrees with the two recommendations.
>
> Defence has made significant progress on capacity and capability building in the ICT project, program and portfolio management areas since the commencement of the Strategic Reform Program. However, more work is required and this activity is already underway.
>
> Defence, through the Chief Information Officer Group (CIOG), has sufficient resources to support military operations and reform activities. Resource constraints are being applied to lower priority, non-reform related ICT activities. CIOG has recently entered into partnership arrangements with five industry specialist companies to provide additional project capacity, in particular to major reform activities such as the next generation HR and financial systems. Resources will continue to be closely managed to ensure high priority reform activities are delivered
>
> Defence remains committed to the delivery of the Strategic Reform Program (SRP) and acknowledges the challenges associated with a reform program of this magnitude. Defence also notes that not all the SRP reforms are dependent on ICT investment for program activities or savings. The SRP is progressing well and exceeded savings targets in its first two years. Defence is committed to managing the complexities of the reform programs and continues to drive ICT reform initiatives to ensure Defence's ICT requirements are met.

Recommendations

Recommendation No. 1

Paragraph 4.86

The ANAO recommends that, to address emerging risks in the delivery of ICT support to Defence business, Defence:

(a) clarify the role of CIOG as an ICT service provider and coordinating capability manager of Defence ICT; and

(b) ensure that Defence program managers and SRP streams adopt a full partnership model with CIOG to deliver relevant Defence portfolio initiatives.

Defence response: Agreed

Recommendation No. 2

Paragraph 4.91

The ANAO recommends that, to improve the portfolio-level view of Defence's enterprise needs and to support the achievement of the challenging goal of managing Defence as a single entity, Defence:

(c) establish an enterprise-wide benefits realisation framework;

(d) ensure it has in place appropriate financial systems to support the effective planning and monitoring of ICT investments; and

(e) develop a consistent, portfolio-wide approach to escalating and treating ICT program and project risks.

Defence response: Agreed

Audit Findings

1. Introduction

This chapter provides an overview of Defence's ICT reforms, including in the context of the SRP. It also discusses portfolio and program management maturity as a framework for establishing, monitoring and assessing ICT improvement. The audit approach, objective and scope are also outlined.

Defence Information and Communication Technology

Introduction

1.2 Information and Communication Technology (ICT) supports the war fighting capability of the Australian Defence Force, Defence's corporate functions and Defence intelligence capability. ICT is essential to Defence's own operations, its operations with coalition partners and allies, and for collaboration across the Government and with industry. Thus effective and efficient ICT services and management are critical to the achievement of Defence's strategic objectives.

1.3 Defence hosts one of the largest ICT networks in Australia.[25] The Defence Information Environment (DIE) connects over 500 Defence sites within Australia and overseas, and incorporates support for 8400 servers, 107 000 workstations,[26] 20 000 laptops, and 15 000 mobile phones.[27] Defence estimates that it cost $1.2 billion in 2010–11 to deliver its highly diverse ICT services across its portfolio. These services range from weapons support systems to payroll, from electronic counter-insurgency to word processing, and from computer aided design to air traffic control management.

1.4 The scale and complexity of the DIE indicates the magnitude of the task of providing Defence with ICT services. The large size of the Defence organisation, its geographical dispersion and its high operational reliance on

[25] According to Defence, its ICT network is the third largest in Australia. Telstra and Optus have larger commercial networks.

[26] About the Chief Information Officer Group, available from <http://www.defence.gov.au/cio/about_ciog/index.htm> [Accessed 10 May 2011].

[27] Department of Defence, Chief Information Officer Group, *Defence Information Infrastructure (DII) Plan – Financial Year 2007–2008,* p. 19. The DIE comprises the information used by Defence and the means by which it is created, managed, manipulated, stored, disseminated and protected. The DIE's two main elements are information domains and information infrastructure, and it encompasses all assets and capabilities involved in the exchange of information by computers and communications across all security domains used by Defence for Military Operations and Defence business.

ICT make it critical for Defence to adopt strategically led, systematic and formal approaches to the management and delivery of its ICT.

The management and delivery of Defence ICT

1.5 The CIOG is the Defence Group responsible for ensuring that Defence has a dependable, secure and integrated DIE that is capable of supporting Defence's military, intelligence and business functions. The CIO leads the Group and, in 2009, was confirmed as the Coordinating Capability Manager for the DIE.[28] This appointment signals Defence's intent to manage ICT in a strategically coordinated way, recognising that ICT management is a specialised function. The CIO's responsibilities include developing the architecture for a single information environment for all Defence ICT systems, and setting ICT standards.

1.6 The Defence organisations that rely on effective ICT services include the three Services of the ADF,[29] the Department of Defence Group functional areas,[30] and the Defence Materiel Organisation (DMO).[31] Defence ICT services are largely supplied by CIOG, as well as the DMO, the Defence Intelligence and Security Group (I&S),[32] and the Defence Science and Technology Organisation (DSTO).[33] The CIOG has an important role in the strategic

[28] The principle role of the Coordinating Capability Manager is to coordinate the generation and sustainment of a communal or shared capability within Defence. This means working collaboratively across organisational boundaries to meet specific capability needs. The Coordinating Capability Manager applies where multiple Defence Groups are involved in a function, and the bulk of the ownership can not be contained to a Group. See Department of Defence, *Defence Information and Communications Technology Strategy 2009*, p. 7.

[29] The ADF is made up of the three Services: Navy, Army, and Air Force.

[30] The Defence Groups are the functional areas and business divisions in the Department of Defence, including: Office of the Secretary and Chief of the Defence Force Group; Vice Chief of Defence Force Group; Joint Operations Command; Capability Development Group; Chief Finance Officer Group; Chief Information Officer Group; Defence Support Group; Intelligence and Security Group; People, Strategies and Policy Group; and Defence Science and Technology Organisation.

[31] The DMO buys and maintains equipment for the Department of Defence to equip and sustain ADF operations. The DMO became a prescribed agency under the *Financial Management and Accountability Act 1997* (FMA Act) on 1 July 2005. The DMO's Chief Executive Officer is directly accountable to the Minister for Defence for its performance and finances, while remaining accountable to the Secretary under the *Public Service Act 1999*.

[32] I&S Group provide direction for the overall planning and management of the Defence Intelligence agencies and the Defence Security Authority. The Defence Intelligence agencies collectively comprise the: Defence Intelligence Organisation; Defence Imagery and Geospatial Organisation; and the Defence Signals Directorate. The Defence Security Authority provides protective security leadership for Defence and conducts all personnel security vetting for the whole-of-government.

[33] DSTO is part of the Department of Defence and has been charged with applying science and technology to protect and defend Australia and its national interests.

planning and management of the DIE, though it is not the sole deliverer of the DIE's capability, which is owned and managed in conjunction with other Defence Groups and Services. Figure 1.1 overleaf shows the common, shared and unique layers in the DIE.

1.7 The two major CIOG-managed network environments are the Defence Restricted Network (DRN[34]), being the largest, and the Defence Secret Network (DSN). Non-CIOG managed network environments include:

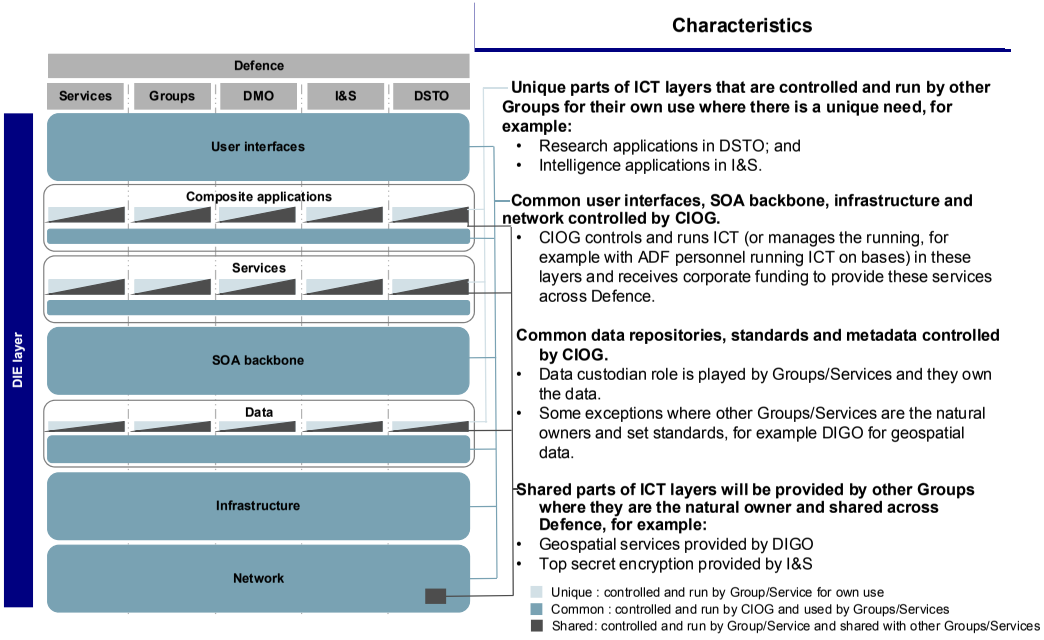
- The Fleet Information Environment (FIE) that resides aboard HMA Ships, mirrors the DRN and DSN and is connected to the fixed infrastructure via satellite. The FIE is managed by Navy.
- Deployed DRN and DSN capabilities connect to their fixed counterparts via satellite and support ADF operations in the field. These deployed components are managed by deployed communications and information systems staff, and supported logistically by the DMO.
- DSTO manages an independent pair of restricted and secret networks, connected via gateways to the DRN and DSN respectively. These networks support the specific requirements of the Defence scientific community.
- A number of highly classified intelligence and surveillance networks exist across Defence, managed by the relevant agency within Defence. Some of these networks have limited one-way connectivity with the DSN.
- A number of unclassified networks are managed by Defence training and education organisations, to support specific training requirements.[35]

[34] The DRN is used for documents up to and including the Restricted security classification level. It is utilised across Australia and internationally by all Defence staff, including staff accessing it remotely. Examples of DRN functionality include: logistics and learning; invoicing and investigations. On the DRN a Defence staff member can request leave, borrow library books and book a flight. The DSN is used for command and control of the ADF, and connectivity of electronic systems up to and including the Secret security classification level. It is utilised across Australia and internationally on ADF operations. On the Secret network, commanders on deployment are linked with their superiors in Canberra by data, voice and video. Intelligence can be disseminated, plans formulated, and orders passed.

[35] Department of Defence, Chief Information Officer Group, *Defence Information Infrastructure (DII) Plan – Financial Year 2007–2008*.

Figure 1.1

The common, shared and unique layers of the Defence Information Environment



Source: ANAO adaption of Defence diagram.

Note: The reference to 'other Groups' in Figure 1.1 refers to Defence Groups other than CIOG.

Note: Services Oriented Architecture (SOA) is an IT architectural approach to designing and developing software in the form of interoperable services.

Improving ICT services in Defence

1.8 Defence ICT services are delivered through a complex mix of diverse systems, with a large number of ICT system owners and stakeholders, to a diverse group of users, via a large number of contracted ICT service providers. Defences estimates that, as of March 2011, some 4500 commercial, government, specialist military and in-house applications were supported and delivered across geographically dispersed, fixed, deployed and mobile networks. This extreme diversity reflects Defence's historical practice of defining and acquiring ICT infrastructure and application services to support individual initiatives and capability needs. Consequently, Defence's ICT has tended to accumulate and operate in a fragmented way, resulting in service gaps, duplication, redundancy and impaired interoperability. As a result, the performance and reliability of Defence ICT has been adversely affected, with support and maintenance becoming difficult and costly.

1.9 These issues were recognised within Defence and raised more broadly when, in 2009, the then Minister for Defence acknowledged both the need for ICT reform in Defence and that it would take time to achieve:

> Defence faces real problems with its own infrastructure. Some of Defence's ICT systems are antiquated and inadequate for Defence's complex operational requirements as a result of being grossly under-funded for years. Some of the department's ICT systems are now too cumbersome, fragile, and costly to operate effectively.[36]

1.10 Notably, four reviews in the period 2007 to 2009 assessed the state of Defence's ICT and all identified the need for Defence to improve its management of ICT.[37] Issues which the reviews found at the time included:

- the need for central management of the Defence-wide ICT spend:
    - the CIO had oversight of less than half of the then estimated $1.2 billion Defence-wide ICT expenditure;

[36] The then Minister for Defence, the Hon John Faulkner MP, speech to the Australia and New Zealand School of Government, *Governance and Defence, Some Early Impressions*, 13 August 2009.

[37] The four reviews are the: *Defence Management Review; Defence Budget Audit; CIO review of ICT;* and the *Defence White Paper – Information and Communications Technology Companion Review*. Refer to Appendix 1 for further information on the four reviews and for information on the *2008 Review of the Australian Government's Use of ICT* (Gershon Review).

- an absence of strategic planning and maintenance of the ICT infrastructure:
    - the DIE supported up to 200 data centres, with Defence finding it difficult to quantify the costs of supporting these facilities. Defence considers that it had under estimated, resourced, and planned for future data centre capability;
    - Defence personnel were required to use multiple desktop devices to enable connection to multiple networks, increasing the amount of hardware, power, and space required; and
    - the age of Defence's network infrastructure (including desktops and monitors) meant that a significant proportion of ICT assets were beyond their effective life, and in many cases were no longer supported by the original equipment manufacturer or under warranty.
- uncoordinated ICT acquisition and sourcing:
    - approximately 4000 different applications were running on the DRN, with very fragmented control over applications, resulting in duplication in application functionality and high software ownership costs;
    - the CIOG ICT spend was mostly (some 85 per cent) on external providers, but it was not strategically managed, as a result of procurement being decentralised; and
    - ICT procurement processes were lengthy and could not keep up with the speed of new technology development, leading to an unacceptable risk of delivering obsolete technology.

1.11 At the time that it released the Defence White Paper in May 2009,[38] the Government announced it would invest more than $940 million over four

[38] Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030 – Defence White Paper 2009*, May 2009. The Defence White Paper outlines the Government's policy, capability and funding expectations of Defence in the period to 2030.

years to reform and remediate the DIE and its supporting infrastructure.[39] This is a significant program of investment and presents a correspondingly difficult management challenge for Defence, particularly given the continuing need to provide and support existing ICT services during the reform period.

The Strategic Reform Program

1.12 The Strategic Reform Program (SRP), announced in May 2009, put into operation the policy direction set by the White Paper. The SRP aims to reform most areas of Defence and generate efficiencies and savings of some $20 billion over the next 10 years. In the 2009–10 Budget, the Government set Defence a fixed funding model to provide additional funding of $146 billion to fully fund the White Paper over 21 years to 2029–30. Under the model, Budget funding to Defence will have 3 per cent average real growth to 2017–18, 2.2 per cent average real growth from 2018–19 to 2029–30 and 2.5 per cent fixed price indexation from 2009–10 to 2029–30, with the 2.5 per cent to be calculated from 2009–10 but applied only from 2013–14. Under these arrangements, the $20 billion gross savings from the SRP and other initiatives will accumulate in the Defence Strategic Investment Reserve for re-investment in higher priority Defence capabilities. Fixed funding applies to all years individually over the 21 year period and cannot be exceeded in any individual year. Defence will continue to seek supplementation for operations on a no-win, no-loss basis.[40]

1.13 The savings are to be reinvested to deliver stronger military capabilities, remediate previously under-funded areas, and modernise the Defence enterprise 'backbone'.[41] The SRP 's three key objectives are to improve accountability, improve planning, and enhance productivity.[42] Responsibility for achieving these objectives lies with 15 SRP reform streams,[43] including an ICT reform stream.

---

39 Minister for Defence, the Hon. Joel Fitzgibbon MP, *Multi-million dollar investment to reform Defence ICT*, Media Release, Parliament House, Canberra, 2 May 2009.

40 See Department of Defence, *Budget portfolio Statements 2009–10*, May 2009, p. 15, and Department of Defence, *Incoming Government Brief,* Circa 2010, p.6-1.

41 Department of Defence, *The Strategic Reform Program – Delivering Force 2030*, 2009, p. 3. The 'backbone' includes facilities and infrastructure, ICT systems, and warehousing and distribution systems.

42 ibid., p. 5.

43 Seven of the streams have costs savings, and there are eight non-saving streams. The 15 SRP streams are set out in Appendix 4.

1.14 The ICT reform stream aims to deliver gross savings of $1.9 billion over ten years, with anticipated additional annual savings of $250 million thereafter. Defence has assessed that to make the required reforms to ICT and generate the required savings will require an up-front investment in ICT reform of $940 million. The performance objectives of the ICT reform stream are to increase the effectiveness of ICT delivery by consolidating data centres; to create a single enterprise architecture;[44] to standardise the Defence ICT environment; and to review the effectiveness of the two-pass approval process for ICT initiatives.[45]

1.15 Other major reform streams of Defence's SRP rely, to a greater or lesser extent, on significant ICT initiatives, supported by successful ICT reform. Accordingly, significant aspects of the SRP require ICT-enabled business transformation, with the attendant potential benefits and risks:

> A fundamental principle [*behind increased investment in ICT*] is that it will deliver better cost effectiveness through the streamlining and amalgamation of corporate support activities…The financial risks associated with IT-enabled business change are due therefore not only to the scale of the programmes and projects themselves, but to the benefits they need to achieve and the pressure to produce return on investment.[46]

1.16 In addition to ICT reform, the provision of effective business-as-usual ICT services, including infrastructure, applications development and sourcing, is important for the success of all other SRP initiatives and business processes, across the 15 SRP reform streams. For example, enhanced productivity is expected from more efficient back office functions through ICT related initiatives, including:

- new capabilities, such as the automation of procurement, security vetting, recruitment, estate management and management reporting;
- a better integrated payroll and personnel management capability; and
- the introduction of a whole-of-Defence enterprise resource management system.

---

[44] Enterprise Architecture (EA) facilitates the alignment of Defence's investment in information technologies with its operational and business needs. It provides a common structure that can be used as a basis for capability planning and the development of consistent enterprise-wide processes.

[45] Department of Defence, *The Strategic Reform Program*, op. cit., p. 6.

[46] United Kingdom National Audit Office, 2006, *Delivering successful IT-enabled business change*, 2006, p. 24.

1.17 Each of these initiatives is governed by a distinct SRP reform stream governance committee, separate from that of the SRP ICT reform stream. Table1.1 broadly outlines the ICT initiatives supporting other SRP streams.

Table 1.1

SRP stream ICT initiatives

Related SRP Stream	Initiative
Logistics	Improved logistics planning, management and execution systems, including Automated Identification Technology (for example the Military Integrated Logistics Information System (MILIS)).
Reserves	Reserves skills database.
Smart Sustainment	Increasing effectiveness and efficiency in maintenance, inventory, and supply chain management.
Non-Equipment procurement	Improved governance arrangements to standardise and streamline buying and contracting practices across Defence Services and Groups.
Preparedness	Refining the Preparedness Management System. Improvements to Defence financial and human resource management systems (for example the Personnel Management Key Solution (PMKeyS) refresh and improvements to Defence Budget and Output Resourcing Information System (BORIS)) to support preparedness.
Intelligence	Restructuring ICT capabilities of the three Defence Intelligence agencies.

Source: ANAO analysis of Department of Defence, *The Strategic Reform Program – Delivering Force 2030*, 2009, especially pages 14, 16, 17, 19, 22 and 23.

1.18 Fundamental reform on the scale of the SRP is a complex undertaking. Over the last 20 to 30 years, Defence has embarked on a number of organisation-wide reform programs, with a limited amount of success.[47] The SRP is pursuing transformation of Defence's business through a fundamental reform of culture, business activity and management, rather than relying mainly on structural change. Defence considers that the SRP represents the most complex change program it has ever undertaken, as it impacts on all elements of its processes and work activities.

[47] The most recent of these experiences was the Defence Reform Program (DRP) conducted from 1997 to 2000. In an October 2001 performance audit of the DRP, the ANAO identified a need for clearer lines of responsibility and accountability, and a better balance between achievement of savings and underpinning reforms.

The Defence Information and Communication Technology Strategy 2009

1.19 Simultaneous with the SRP, CIOG has progressed strategic planning for all aspects of Defence's ICT services, including those that have not been brought within the scope of the SRP. The DICT Strategy, released in November 2009, is a statement of Defence's strategic intent with regard to its future ICT environment. The DICT Strategy was developed in response to the recommendations of the *Defence Management Review 2007* (Proust Review) to:

> address shortcomings in governance, planning and control frameworks for ICT.[48]

1.20 The DICT Strategy outlines the role of the CIO, and Defence's strategic priorities and the role of ICT in achieving them. It also identifies the need for an investment of around $940 million over four years,[49] and expected savings of $1.9 billion[50] over 10 years and around $250 million per year thereafter. The DICT Strategy describes the desired end state of the DIE as follows:

> The DIE will be one network connecting fixed and deployed locations built on a single set of standards and products. It will encompass all security levels and will determine that the right person has the right authority to access information.
>
> A typical desktop set up available to all Defence sites will be a single screen connected to a network that can display multiple security sessions. Secure voice and video will be available to the desktop in most fixed and deployed locations. Wireless networks will also be considered in appropriate locations.
>
> Deployed commanders and decision makers will have a single view of the battle space through a Common Operating Picture accessing a wide range of data from sensors and sources.
>
> Finance, payroll and personnel information will be easily accessed, manipulated and aggregated by authorised Defence staff. New capabilities such as the automation of procurement, personnel and pay administration, vetting, recruitment, estate management and performance reporting will be progressively introduced.

---

48 Department of Defence, *Defence Information and Communications Technology Strategy 2009*, p. 5.

49 The SRP states that around $700 million will be required.

50 The DICT Strategy does not state whether these savings are gross or net; however, the SRP contains a target of $1.9 billion gross, costs of $708 million, and net savings of $1.24 billion for the ICT Stream over 10 years.

1.21 The DICT Strategy is arranged around four strategic imperatives, each with a number of strategic elements to be implemented through individual ICT initiatives, as shown in Figure 1.2.

1.22 Supporting the DICT Strategy is Defence's *Single Information Environment (SIE) Architectural Intent 2010*. The SIE outlines a conceptual view and intent for the single information environment envisaged by the DICT Strategy. The SIE envisages a disciplined approach to ICT planning, design and implementation through an enterprise architecture model that standardises the infrastructure and technical standards, implemented principally at the requirements phase of defining future capability. It is a first step toward establishing the direction and enforcement of Defence-wide ICT standards.

1.23 Since the release of the DICT Strategy, CIOG has developed the Defence ICT Program Design Manual (PDM), aimed at describing the governance arrangements, program disciplines and plans to facilitate the implementation of Defence's ICT reform initiatives.[51] The PDM represents a further development of strategic planning within CIOG, including the SRP ICT Reform Stream, the ICT aspects of other SRP Streams and the intent of the DICT Strategy, linking these together to form a program of work. The PDM has provided Defence with an opportunity to clarify what needs to be done to implement its ICT reforms and ICT-enabled business transformation under the SRP.

[51] The PDM comprises 275 PowerPoint slides for use within CIOG.

Figure 1.2

DICT Strategy: strategic imperatives, elements and initiatives

Strategic Imperatives	1. Optimise Defence ICT Investment	2. Closer Stakeholder Engagement & Alignment	3. Provide Agreed, Priority Solutions	4. Strengthen ICT Capability
Strategic Elements	• Improve ICT cost transparency and stakeholder communication • Prioritise for effective ICT spend • Optimise project operations and efficiency • Harmonise with whole-of-government initiatives	• Improve alignment between stakeholder needs and ICT capabilities • Align ICT organisation with stakeholders • Become easier to work with • Design solutions collaboratively with stakeholders • Implement Defence-wide ICT Governance	• Stabilise and secure ICT • Consolidate, standardise and optimise ICT • Address new ICT requirements • Leverage emerging technologies to address new business needs • Create and adopt an Enterprise Architecture	• Energise the culture • Strengthen ICT leadership • Improve processes and tools • Professionalise the workforce • Leverage vendors and sourcing • Leverage scale and effective resource planning and management
Initiatives	• Consolidate data centres • Reduce 'Time to Market' ICT two-pass process • Implement a single secure desktop • Develop Defence's enterprise architecting capabilities • Implementing a Services Oriented Architecture • DIE simulation and modelling • Centralised services – deliver Distributed Computing	• New stakeholder engagement model • Improved sharing and access to services with key allies • Specialist business solutions design capability	• Information management • Deliver unified communications • High speed strategic communications network (JP 2047) • Analysis of disruptive technology	• Sourcing strategy • Investing in people • IT service management • ICT reform portfolio management • CIO as Coordinating Capability Manager • Infrastructure remediation

Source: ANAO analysis.

Integrating Defence's strategic imperatives for ICT reform

1.24 Taken as a whole, the outcomes of recent ICT reviews and strategic planning processes in Defence, listed in Table 1.2, set out a framework for Defence's current approach to the reform of its ICT. These reviews and strategic plans outline the policy, strategic aims and objectives, operational concepts and guidance, and provide the basis for Defence's ICT capability development and improvement.

Table 1.2

Defence ICT strategic guidance documents

Purpose of strategic guidance	Document
Policy Direction	*Defence White Paper 2009 – Defending Australia in the Asia Pacific Century: Force 2030*
Defence management priorities	*The Strategic Reform Program: Delivering Force 2030* (SRP)
Service-level strategy	*Defence Information and Communication Technology Strategy 2009* (DICT Strategy)
Information environment strategy	*Single Information Environment (SIE) Architectural Intent 2010*
Activities/Tasks	*Defence ICT Reform Program Design Manual* (PDM – the DICT Strategy implementation plan)

Source: ANAO analysis.

1.25 It is important that Defence has in place mechanisms to ensure ICT resources and efforts are directed towards achieving the organisation's business priorities, ideally by linking ICT decisions to Defence's business requirements and by setting ICT priorities based on Defence business priorities. On this basis, the SRP and DICT Strategy together play a key role in aligning Defence's ICT approach with its strategic intentions and objectives. Defence informed the ANAO in October 2011 that:

> The SRP is a key enabler of delivering [*Force*] 2030 through fundamental and sustainable changes to the way Defence does business. The ICT Strategy articulates CIOG's approach to delivering on its responsibilities to provide ongoing ICT services to the Defence organisation, including the approach to Reform activities.

1.26 The Defence ICT Reform Program is to be the principal vehicle for the management and delivery of the DICT Strategy. The seven key outcomes of the

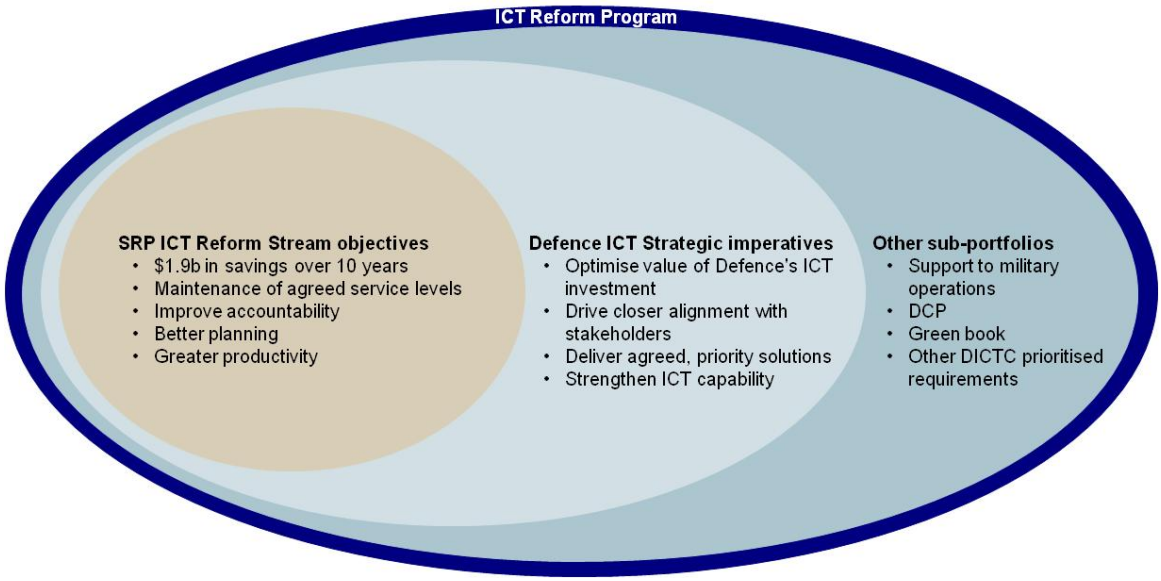
DICT Strategy encompass, at a high level, proposed ICT activities set out in the DICT Strategy, aligned with the ICT stream of the SRP, and intended to be:

> managed as components of a single Defence ICT Work Plan under the ICT Reform Stream [*of the SRP*].

1.27 Figure 1.3 sets out the other influential sub-portfolio drivers on Defence ICT strategic intentions and objectives which, in addition to the SRP and DICT Strategy, make up the integrated ICT reform program. Sub-portfolio influences include major capital equipment initiatives derived from the Defence Capability Plan (DCP),[52] and ICT infrastructure support to Defence facilities derived from the Green Book,[53] which includes a significant ICT component.

Figure 1.3

Delivering on Defence ICT strategic imperatives: integrated ICT reform program



Source: Department of Defence.

1.28 At this high level, Defence's integrated ICT reform agenda is essentially threefold: the rationalisation, standardisation, replacement and maintenance of

[52] The DCP outlines the major capital equipment proposals that are currently planned for Government consideration over a ten-year planning horizon. The DCP provides key information for Parliament, Defence industry and the Australian public on Defence's Capital Acquisition Plans.

[53] The Green Book is a program of approved Defence capital facilities projects. Available from <http://www.defence.gov.au/im/support/mcf_program/mcf_program_development.htm> [Accessed 24 October 2011].

existing systems; the development and deployment of new systems; and, alongside these reforms, the continued delivery of normal day-to-day ICT services at agreed service levels.

Audit approach

Audit objective and approach

1.29 The objective of the audit was to assess the development of Defence's oversight and management of its portfolio of ICT investments and projects. The high level audit criteria were that Defence has in place:

- governance, strategic processes and decision-making structures that set out, prioritise and coordinate the integrated ICT reform portfolio and programs;
- ICT risk management and capacity to identify and plan to achieve the benefits of its SRP ICT stream reforms (including methodologies to measure the realisation of savings and non-savings benefits);
- the appropriate level of portfolio and program management maturity; and
- improvement efforts that are generating the ability to deliver the ICT services capacity required to support the SRP.

1.30 As the implementation of the SRP's ICT-enabled reform initiatives is still in its early stages, the audit did not generally extend to assessing the realisation of benefits, although from a budgetary perspective it should be noted that each year, over the period 2009 to 2019, the Defence ICT budget will be reduced to achieve the total gross savings of $1.9 billion required under the ICT stream of the SRP (see also paragraph 1.12). This places additional pressure on CIOG to become more efficient and effectively manage its risks. The status of the key integrated ICT reform initiatives is included in Appendix 2.

1.31 The ANAO's focus was on remediated or new Defence ICT capability resulting from the integrated ICT reform program. For the purposes of this audit, the management and sustainment of ICT business-as-usual, existing

DMO military equipment and support infrastructure,[54] the DSTO scientific community and I&S top secret and highly classified networks were not included. DMO, DSTO and I&S were only included to the extent that they had new ICT capability initiatives, or where they were a stakeholder of one of Defence's business applications[55] that was part of the IPW. The project management of individual ICT projects was also out of scope.

1.32 The audit was conducted in accordance with ANAO auditing standards at a cost to the ANAO of approximately $585 000.

[54] DMO supports a diverse range of equipment including aircraft, ships, vehicles, weapons, sensors and the electronic systems and in-service command and support communication systems. DMO military equipment and support infrastructure connects to the Defence information infrastructure via CIOG-managed interfaces and is supported by a CIOG-managed help desk.

[55] There is a range of business and corporate applications that are utilised by all of the Defence organisations. For example, PMKeyS (the core human resource management information system, and authoritative personnel management record for all Defence personnel) manages payroll for Defence APS employees, including DMO employees.

2. Governance structures and decision-making processes

This chapter examines the Defence ICT governance structure and strategic decision-making processes. This includes the support given to senior decision-makers in Defence when considering key strategic ICT issues, in order to make informed decisions and set priorities for ICT in line with business objectives.

Introduction

2.1 In the context of the 2009 Defence White Paper and the SRP, high priority has been placed on improving Defence ICT capability. This, together with the complexity of management arrangements across the organisation's Groups and Services, reinforces the importance of Defence having in place effective governance structures and processes to support decision-making on key strategic ICT issues, including in relation to setting priorities. In June 2008, the then Secretary of Defence acknowledged that longstanding problems in areas such as ICT pointed to:

> failings in the governance and accountability arrangements that we must get right if we are to perform to the highest level while also conforming with the law and Government policy... On the governance side, we're overhauling the process of how we set priorities and assign resources—replacing a bottom-up, uncoordinated approach with one led by [*the Chief of the Defence Force*] and [*the Secretary of Defence*] that looks across the enterprise and takes the hard decisions about where investment will get the most return.[56]

2.2 This statement evidences commitment at the most senior level in Defence to establishing effective governance structures and to taking a portfolio-wide view on investment. Between then (2008) and this audit, Defence has taken steps towards achieving portfolio-level oversight of the evaluation, prioritisation, and monitoring of its ICT investments. From a (self-identified) low base, Defence is aiming for a state in which strategic ICT investment decisions are made at the most senior level and program managers are accountable for overseeing the implementation of ICT programs, in order to deliver the outcomes and benefits envisaged.

[56] Warner, N (Secretary Department of Defence), *256,800 paper hand towels: Mending Defence's broken backbone*, Speech to the Lowy Institute for International Policy, 10 June 2008.

2.3 To assess the progress Defence has made in establishing portfolio-level governance and decision-making processes, the ANAO examined the following key areas:

- strategic/portfolio level governance structures impacting on Defence ICT; and
- strategic/portfolio level decision making about ICT.

Governance structures for Defence's ICT

2.4 Defence has established a committee structure as part of the governance arrangements to direct and oversee ICT investments. Figure 2.1 shows the relevant Defence Senior Management Committees, the ICT governance and decision-making structure, and the internal SRP ICT governance structure.

2.5 The principal committees in Defence's ICT governance structure are the Defence Information Communications Technology Committee (DICTC) and the Defence Information Environment Committee (DIEC). The DICTC was established as Defence's pre-eminent ICT committee in August 2008.[57]

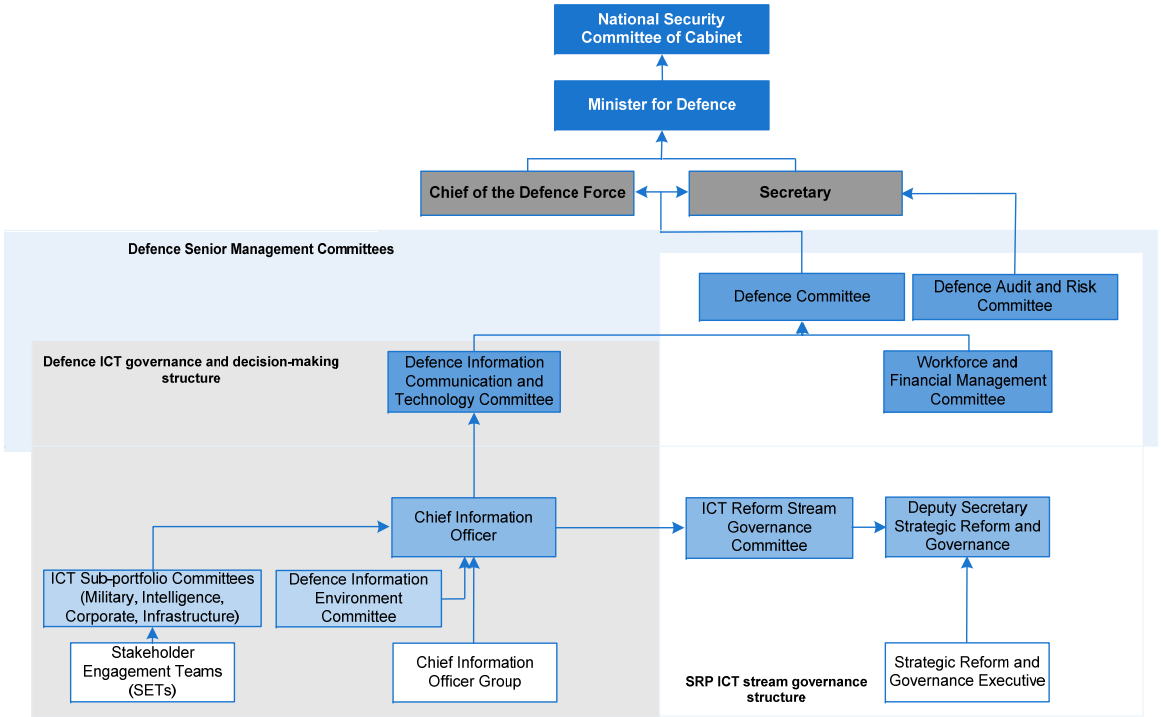
2.6 The DICT Strategy identifies the DICTC's role as to provide strategic direction on the planning, expenditure and allocation of ICT resources across Defence. The DICTC was to provide strategic and financial ICT governance from a Defence-wide perspective, adjusting sub-portfolio budgets and activities in response to competing priorities.[58] The DICTC has been an active forum, meeting on 24 occasions between July 2008 and August 2011.

[57] The DICTC is co-chaired by the Secretary of Defence and the Chief of the Defence Force and its members consist of Three Star, or Band Three Senior Executive Service staff.

[58] Department of Defence, *Defence Information and Communications Technology Strategy 2009*, p. 28. Defence informed the ANAO in October 2011 that 'financial governance of ICT from a Defence perspective is the role of the Workforce and Financial Management Committee, not the DICTC.'

Figure 2.1

Defence Senior Management Committees and ICT governance and decision-making structure, October 2011



Source: ANAO analysis.

2.7 The DIEC is subordinate to the DICTC, and was formed as a consultative group and a forum to consider ICT stakeholder and user issues, as well as ICT issues related to the SRP.[59] Compared to DICTC, the DIEC has a history of inactivity. After being constituted in August 2008 it became inactive until September 2010. The DIEC subsequently met six times from September 2010 to September 2011, however in October 2011, Defence informed the ANAO that:

> The role of the DIEC has not proven effective and so the three star/Band 3 ICT/Intelligence Reform Stream Governance Committee[60] was re-activated in April 2011 to provide governance of the ICT Reform Stream.

2.8 At that time, Defence also informed the ANAO that the role of the DIEC had been clarified and its current role was to:

(a) consider and develop whole-of-Defence advice for DICTC in relation to the ICT planning cycle; and

(b) in relation to ICT Reform Stream initiatives:

- de-conflict priorities within the Integrated Plan of Work;
- coordinate Group perspectives on Defence's information capability before consideration by the DICTC; and
- identify interdependencies with the ICT stream across the other [*SRP*] reform streams.

ICT Sub-portfolio Committees representing the Groups' and Services' ICT priorities and requirements

2.9 In addition to the DIEC, a number of constituent committees have been formed to support and feed into strategic Defence-wide ICT portfolio decision-making.[61] The function of these constituent committees is either to represent the Groups' and Services' ICT priorities and requirements, or to govern the SRP ICT reforms.

2.10 In order to manage its ICT investments, Defence has divided its business needs into four sub-portfolios: Intelligence, Military, Corporate and

---

[59] Not all ICT related proposals or policies are expected to be considered by the DIEC before being presented to DICTC for endorsement.

[60] The ICT and Intelligence Reform Stream Governance Committee is discussed in paragraph 2.15.

[61] The constituent committees include the Sourcing Steering Committee, the Infrastructure Sub-portfolio Committee and the Enterprise Architecture Committee.

Infrastructure. The Intelligence, Military and Corporate sub-portfolios each have a committee that is responsible for implementing the structure that the DICT Strategy expected to provide for improved cost transparency and stakeholder engagement.[62] This includes ensuring a holistic view of ICT capabilities for their representative sub-portfolios, enabling a better understanding of stakeholder needs, and providing a voice to the ICT customer.

2.11 After having been established in 2010, the Military and Corporate sub-portfolio committees set about determining their working arrangements. However, Defence informed the ANAO in October 2011 that:

> The first meeting of the Military sub-portfolio committee was held in May 2010 to articulate and agree IPW priorities, with a follow up meeting held in July 2010. The Military sub-portfolio committee has not formally met since this time due to delays in establishing a way forward with this financial year's IPW. The Military Stakeholder Engagement team has continued with one-on-one engagement with [*CIO*] Group point of contacts and at Deputy Service Chief level.

2.12 The Military, Intelligence and Corporate sub-portfolio committees are each supported by a Stakeholder Engagement Team (SET) established within CIOG. The role of each SET is: to be responsible for the overall ICT service delivery to their stakeholders; facilitate the development of strategic ICT demand forecasts; to seek to ensure that stakeholders' business needs are represented; and assist with understanding stakeholder requirements and the development of proposals for new ICT capabilities.

2.13 The SETs have been operating since early 2009, before the sub-portfolio committees were established. In particular, the Military SET was actively representing the Services' agreed ICT prioritised initiatives to DICTC in March 2009. Between March and June 2010, representatives from the Military, Intelligence and Corporate sub-portfolio committees consulted with their respective groups on their ICT priorities and refined the Defence ICT portfolio work program (see Table 2.1). The establishment of the sub-portfolio committees and the SETs to support them is aimed at implementing the DICT

[62] The Infrastructure Sub-portfolio is owned by the Chief Technology Officer and operated within CIOG, therefore is not supported by a Sub-portfolio Committee or a Stakeholder Engagement Team (SET) but by the CIOG Executive. The purpose of the Infrastructure Sub-portfolio is to enable the ICT infrastructure (physical and technological) to support the quality of the ICT activities delivered by the other sub-portfolios.

Strategy's imperative for closer stakeholder engagement and alignment. These constituent committees facilitate stakeholder engagement and contribute to the review of controls over the development, evaluation and screening of ICT initiative proposals before they are considered by DICTC.

SRP ICT stream governance

2.14 Defence's SRP implementation plan was endorsed by the Government in March 2010. The SRP implementation plan requires each SRP stream to be lead by a Senior Executive Stream Leader who also chairs the relevant stream Governance Committee.

2.15 A joint ICT and Intelligence Stream Governance Committee was formed and initially co-chaired by the CIO and the Deputy Secretary Intelligence and Strategy. At its first meeting in June 2009, the Committee agreed that the DICTC was the forum in which ICT initiative and resource priority decisions would be made, and that the ICT and Intelligence Stream Governance Committee would focus on the SRP ICT stream reform program. This effectively created two separate decision-making forums for considering the allocation of ICT resources and for prioritising ICT initiatives, some of which support more than one SRP stream.

2.16 The Deputy Secretary Strategic Reform and Governance (DSSRG) attended the ICT and Intelligence Stream Governance Committee meetings. Given the DSSRG's responsibilities for the high-level integration, coordination and oversight of the SRP, the ICT Stream Governance Committee meetings provided a forum to provide the DSSRG with an update on the ICT reform program (including scope, priorities, deliverables, timelines and savings), as a standing agenda item.

2.17 The operation of the ICT and Intelligence Stream Governance Committee is intended to support the DSSRG acquit his responsibilities to the three Defence Senior Management Committees that have been tasked with SRP governance responsibilities, as follows:

- *Defence Committee (DC):* which monitors overall progress on reform;
- *Defence Audit and Risk Committee (DARC):* which is responsible for monitoring the SRP and providing an annual assurance sign-off on achievement of savings targets; and
- *Workforce and Financial Management Committee (WFMC):* which is responsible for deciding upon investment proposals on reform

initiatives, considering the overall value to Defence and the SRP in a whole-of-Defence context, and undertaking workforce planning and allocation decisions.

2.18 However, after holding three meetings in 2009, and one in March 2010, the ICT and Intelligence Stream Governance Committee then went into abeyance, with the DIEC subsequently noting in September 2010 that it would undertake the role of the Senior Executive Governance Committee for the ICT and Intelligence Stream of the SRP.[63] Defence informed the ANAO in December 2011 that:

> the ICT and Intelligence Stream Governance Committee was reactivated in 2011.

ICT Portfolio Management Office

2.19 A Portfolio Management Office (PMO), whether permanent or virtual, is commonly responsible for managing change within an organisation. Usually established at the strategic level, a PMO is generally responsible for:

- comprehensive program planning;
- change and risk management;
- coordination of project delivery;
- measurement of results; and
- business/internal collaboration.[64]

2.20 Originally, Defence established two separate PMO's to deal with the ICT reform Program and the SRP ICT stream. In October 2011, Defence informed the ANAO that:

> The initial ICT Reform Stream PMO was set up in July 2009 to design the ICT Reform Program. This was merged with the existing CIOG PMO in July 2010 to refocus efforts on the IPW.

2.21 The responsibilities of the merged ICTPMO include prioritising ICT investment proposals through coordinating with the SETs and consulting with

---

[63] The May 2010 DC meeting revised SRP governance arrangements, with Band 2 Senior Executive committees replacing the former Band 3 Senior Executive committees. The transition to the new arrangements was to occur over a 12 month period when the streams were considered mature enough.

[64] Whitfield, J; Greener, S. 2009, 'Programme & PMO Governance challenges: Best & worst practice examples'. Gartner Inc.

sub-portfolio committees, the DIEC, and the DICTC; developing the ICT investment program; and ensuring that investments are aligned with current and future Defence Service and Group business needs. The ICTPMO is also responsible for maintaining the master schedule and managing program-level dependencies. Defence informed the ANAO in December 2011 that:

> Defence recognises it has a complex accountability system and is in the process of implementing the recommendations from the *Review of the Defence Accountability Framework*, January 2011.

Strategic ICT management

2.22 Effective strategic management of ICT is often a necessity for success in contemporary business, including that of public sector agencies. This imperative is heightened in the current circumstances, where Defence is undertaking, through the SRP, significant elements of an ICT-enabled business transformation aimed at improving performance and generating savings of some $20 billion over 10 years.

2.23 To adequately inform senior management's decisions on resource allocation for ICT, including on ICT investment, it is important that a strategic prioritisation process is in place that reconciles the needs of the different constituents and ensures that ICT spending reflects Defence's strategic priorities.

2.24 Investments in ICT initiatives need to be considered on the basis of their individual merit in the context of their fit in the current ICT portfolio of commitments, so that new commitments are consistent with capacity. The importance of a systematic and consistently applied method to prioritising ICT initiatives is emphasised when coupled with finite ICT resources.

2.25 An effective and consistently applied ICT investment approval framework is an important foundation for portfolio management. Acquiring, analysing and scrutinising information on ICT initiatives is a fundamental part of the approval framework, and assists with the prioritisation process. The type of information required to prioritise initiatives accords to criteria such as strategic alignment, options, cost, resource availability, risk, benefits, and the configuration to the Defence enterprise architecture.

Defence's ICT budget and expenditure

2.26 Funding is an essential resource that is a key focus when initiating and monitoring ICT initiatives and an ICT portfolio. Generally an entity's ICT

strategic decision-making includes the consideration of how much and where to invest in ICT. In Defence's context this involves settling the responsibility for deciding the appropriate aggregate annual spending in the different areas of sustainment and investments.

2.27 Before 2007, Defence had a fragmented, decentralised ICT environment focussed largely on sustainment activities. Defence informed the ANAO in December 2011 that its first CIO was appointed in 2007 with the initial focus on assessing the state of the Defence Information Environment. Prior to mid-2008, Defence had not collected and collated the data required to make a soundly based estimate of its organisation-wide ICT expenditure. Following a request by the DICTC in July 2008, CIOG gathered data from Defence's financial systems and the Groups and Services to develop such an estimate. CIOG reported to the DICTC that Defence's estimated total annual expenditure in 2008–09 on ICT was $1.6 billion.

2.28 The difficulties of estimating ICT expenditure are illustrated by the subsequent revision down of estimated 2008–09 expenditure from $1.6 billion to $1.2 billion, on the basis of more reliable information obtained by CIOG through surveys conducted by consultants.

2.29 Defence informed the ANAO in October 2011 that CIOG's collection of data from Groups and Services, as part of the Defence ICT Costing Baseline activity, has been refined each year to improve confidence in the data. CIOG's current knowledge of the Defence-wide ICT systems and expenditure, while the best available consolidation to date, is incomplete, relying in part on unverified estimates and other information provided by Defence Groups, Services, and external consultants. Defence informed the ANAO in December 2011 that:

> Outside CIOG, Defence is a highly fragmented organisation with respect to ICT spend. CIOG has already made efforts to optimise its ICT spend; it is unlikely that even this baseline level of cost efficiency has been achieved in other Groups where ICT spend is controlled independent of CIOG, because of the smaller scale.

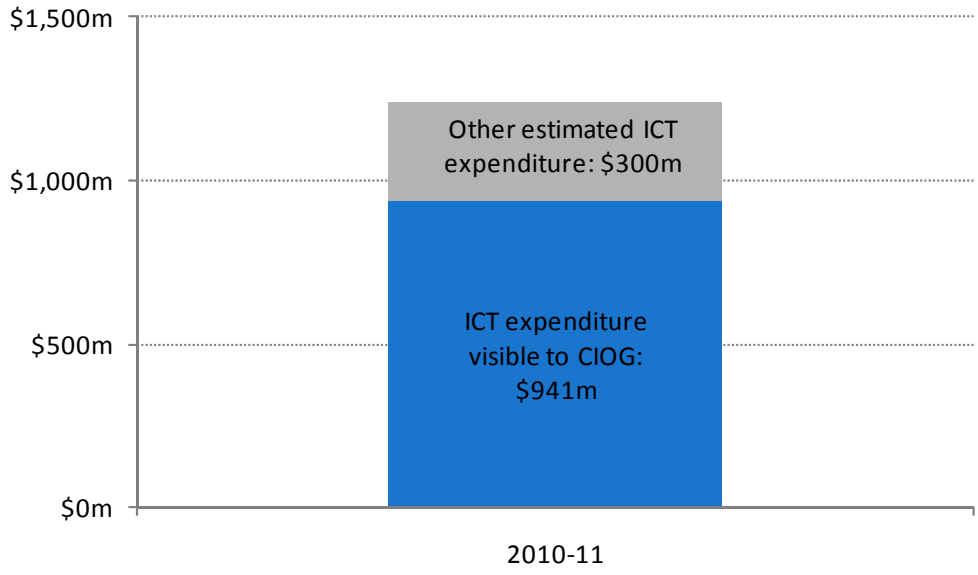
2.30 At the time of this audit, CIOG had direct visibility of some 75 per cent of Defence's ICT expenditure, which is a notable improvement on the situation at May 2009, when CIOG had visibility of less than half of Defence's ICT expenditure. Defence informed the ANAO that the improvement was due largely to:

improved financial reporting of ICT, the Defence ICT Costing Baseline activity, which is now in its third year, and the ongoing maturing governance and consolidation of ICT infrastructure and software licences.

2.31 However, as shown in Figure 2.2, some $300 million of Defence's estimated $1.2 billion ICT expenditure in 2010–11 was not directly visible to CIOG. While Defence's financial reporting of ICT has improved, the $300 million estimated expenditure includes information provided by Defence Groups and Service entities that is not necessarily compiled, recorded or calculated on a consistent basis. The lack of consistent Defence-wide ICT financial data has meant that, to estimate future expenditure and likely ICT savings, Defence has, in some cases, relied on data provided by consultants using proprietary estimation techniques that Defence is not in a position to verify or validate. Defence therefore has a less than complete view of the information needed to effectively manage its ICT, plan future systems, and fully deliver the savings necessary to support the White Paper targets.

Figure 2.2

Defence's estimated ICT expenditure, 2010–11



Source: ANAO analysis of Defence data.

ICT budget oversight and management

2.32 From as early as August 2009, Defence was aware that the responsibilities for overseeing and coordinating its organisation-wide ICT

expenditure and budget were not clear. At that time, the DICTC considered CIOG's first estimates of the extent and focus of Defence's organisation-wide ICT expenditure for the financial year 2008–09. CIOG advised DICTC that, while it was able to provide an estimate of some $922 million total expenditure for ICT activities within its immediate view, it could give only a very approximate estimate of some $300 million total additional ICT expenditure by all other Defence groups, and could not readily identify ICT capital expenditure or depreciation expenses for these groups. As a result of assembling these estimates, CIOG identified a number of concerns, including:

- limited visibility of expenditure on ICT projects and sustainment outside of CIOG;
- a lack of consistent metrics to compare projects and measure complete project cost;
- no standard business case metrics for determining the Net Present Value and Net Personnel Operating Costs[65] of projects or sustainment activities;
- no standards for financial measures or consistent risk measures for ICT projects;
- the lack of an explicit linkage between the ICT expenditure and Defence priorities; and
- the absence of a single view of the ICT spend across Defence.

2.33 DICTC's next recorded consideration of Defence's organisation-wide ICT expenditure related to a ten-year financial budget forecast against the Defence ICT work program, presented to the DICTC by CIOG in October 2009.

2.34 The ANAO notes that DICTC has operated with only limited visibility of Defence-wide ICT costs and budget, and has not been well-placed to acquit the primary responsibility for ensuring that ICT portfolio expenditure is

[65] Net Personnel and Operating Costs (NPOC) reflects the net difference between the cost estimates to operate a new, upgraded or replacement capability and the funding guidance available as an offset in the Defence Management and Finance Plan to operate the current capability, across all affected Groups. NPOC costs include, but are not limited to, maintenance support costs, spares provisioning, fuel, explosive ordnance, infrastructure operating costs, and associated personnel costs including training required to operate, manage and support the capability, system or equipment from acceptance into service through to its disposal.

aligned with Defence priorities, as set out in the *Defence Information and Communications Technology Strategy 2009*:

> At a strategic level, the DICTC provides the strategic and financial governance from a Defence-wide perspective, adjusting sub-portfolio budgets and activities as needed.
>
> …DICTC will continue to consider, review and prioritise all ICT initiatives and expenditure across Defence. All ICT funding decisions will be made within the context of a single Defence-wide ICT portfolio, reflected by a unified Defence ICT workplan and implemented by the Defence-wide ICT workforce.[66]

2.35 Responsibility for internal ICT funding decisions and for allocating and prioritising resources for ICT initiatives passed de facto to Defence's Workforce and Financial Management Committee (WFMC), another senior Defence committee with membership common to the DICTC but without direct representation from CIOG. This arrangement was formalised by Defence in August 2011, almost two years after it was raised with the DICTC. Defence informed the ANAO in October 2011 that:

> Oversight of Defence's ICT budget is managed through the normal departmental budgeting processes and regular consideration by the WFMC.
>
> The WFMC is the appropriate forum for consideration of Defence's organisation-wide ICT expenditure, not the DICTC. On 16 August 2011, Secretary and the CDF (in WFMC) directed the CIO to provide WFMC with a holistic view of the activities, funding requirements and potential offsets to fund the ICT reform program.
>
> The membership of the DICTC and the WFMC has significant overlap, ensuring that the key Departmental Executives have a complete picture across ICT and the financial status of the Department.

2.36 The ANAO notes that the common members of the DICTC and the WFMC are the Secretary and CDF. CIOG continues to report to and support the DICTC, but has no formal linkage to the WFMC (see Figure 2.1).

ICT portfolio prioritisation

2.37 In July 2008, in accord with the methods for managing Defence-wide ICT initiatives that were in place in Defence at that time, CIOG drew up a

[66] Department of Defence, *Defence Information and Communication Technology Strategy 2009*, pp. 8, 17 and 28.

work plan consisting of 1104 initiatives. This initial work plan was presented to the DICTC in July 2008. Subsequently, in November 2008, the DICTC agreed to the creation of a single portfolio of ICT investments and spending across Defence. To help align ICT investments decisions with Defence's strategic objectives, the DICTC set ICT spending and investment priorities:

- *Priority 1*: Sustainment of the current ICT environment and capabilities (with sustainment of military command and control, and systems being used to support military operations, having the highest priority within this category).
- *Priority 2*: Delivering government directed capabilities (such as those described in the DCP, the Green Book and specific business systems).
- *Priority 3*: Prioritised requirements determined by Groups and Services.

2.38 The intention was to facilitate the making of ICT investment decisions, and the relative prioritising of individual ICT initiatives, such that the initiatives selected for funding made the best use of the available resources. Defence had ICT initiatives in progress at varying levels of maturity and, as shown in Table 2.1, in July 2009, DICTC considered the ICT work program (called the Integrated Plan of Work–IPW) in accordance with the priorities it had set in November 2008.

Table 2.1

Development of Defence's ICT Integrated Plan of Work

Date that the work program was presented to DICTC	Approximate number of initiatives listed	How initiatives were categorised	Key changes
July 2008	1104	Initiatives classified against seven different categories and five priority levels ratings.[(a)]	–
July 2009	345[(b)]	Initiatives classified against the three priority areas.	Initiatives grouped for the first time against the three priority areas.
March 2010	64	Initiatives classified against the first and second priority areas.	Priority 3 removed and placed on a pressure list.
June 2010	97	Initiatives classified against the first and second priority areas.	Initiatives were added after consultation with the sub-portfolios. The pressure list with Priority 3 initiatives was not presented.
October 2010	99	Initiatives classified against the first and second priority areas.	Initiatives were listed as: In-flight; or Scoping.[(c)]

Note: (a) Six of the categories were mandatory. The one category that was discretionary included the requested initiatives and tasks from the Defence Groups, with 61 per cent of the listed initiatives recorded against this category. A further 23 per cent of the listed initiatives had not been categorised.

(b) The plan also notes that there were over 1100 additional ICT activities registered on the Defence Information Environment work plan that were not included.

(c) In-flight initiatives were either underway or about to start. The scoping projects were broken down further into those initiatives that were scheduled for scoping and unlikely to commence in 2010–2011, and initiatives that were to be incorporated into the 2011–2012 planning cycle.

Source: ANAO analysis of Defence documentation.

2.39 Table 2.1 also shows the refinement and development of Defence's single portfolio of ICT investments and spending at successive DICTC meetings. The ICT work program was discussed by the DICTC at 11 of its 17

meetings between July 2008 and October 2010, including five occasions on which the DICTC considered the IPW.[67]

2.40 However, much of the IPW comprised work that was already in progress (including business-as-usual) so that, between July 2008 and October 2010, the DICTC actively considered some 30 per cent of the ICT initiatives that were listed in the IPW. Defence informed the ANAO in October 2011 that:

> When the IPW was first established, existing activities were included automatically. Only new projects were presented to the DICTC for approval. Sustainment activity does not require DICTC approval and so the DICTC's governance of the IPW was in relation to additional activity (i.e. projects) not already being done by CIOG as part of its role of provider of ICT to the Defence organisation.

2.41 Limitations on the completeness and reliability of the ICT management information available on Defence ICT resources hindered Defence's ICT planning processes, and it was difficult for Defence to optimise its ICT planning decisions. For instance, the DICTC's Military Sub-portfolio Committee observed in May 2010 that balancing ICT initiative priorities was a difficult undertaking without a more detailed program view that outlined ICT resources over time, to enable a more informed discussion of proposed trade-offs.

2.42 The SRP was released in June 2009, and the SRP ICT reform initiatives were subsequently allocated to the Priority 1 category of the IPW. In July 2009 the Secretary and CDF directed that no expenditure on ICT was to occur in any part of Defence unless it was in accordance with the DICTC priorities.

2.43 By March 2010, the ICT Stream Governance Committee, in its role governing ICT as it relates to the SRP, had also begun to consider the IPW. The committee raised concerns about the inclusion of some SRP projects on the IPW Pressures List rather than in the IPW itself. The Committee agreed that savings-related projects should be prioritised over projects without identified savings, and highlighted the requirement for all SRP projects to be included in the IPW.

[67] DICTC discussions on the ICT work program included refining the work program by bundling initiatives into business groupings, developing ranking criteria for Priority 3, better understanding the workforce requirements and limitations, detailing the cost of initiatives and developing the work plan towards a ten year funding view.

2.44 In March 2010, the ICT Stream Governance Committee noted that CIOG was short of 350 employees to deliver the IPW, and that further work was required on the projects listed on the IPW to ensure that there was an appropriate prioritisation of projects, and that new capabilities were distinguished from projects that were enhancements to existing systems which provided sufficient capability. Defence informed the ANAO in December 2011 that:

> On each occasion the IPW was presented to the DICTC between July 2008 and August 2010, the accompanying brief noted that the work program was oversubscribed and that the CIOG's available resources were insufficient to meet all the requirements of the IPW.

2.45 The February 2011 internal Defence ICT Reform Strategic Assurance Review confirmed that senior Defence business stakeholders saw the over-commitment of resources across the ICT portfolio as a major challenge, and that resource capacity and allocation issues were the most significant risk to the reform program. The review also reported that demand management and prioritisation were not functioning well, and there was no decision-making on cross-Group trade-offs.

2.46 Appropriate planning and prioritisation of initiatives is important to achieving an optimal balance between ICT reform activities and business-as-usual. Defence advised the ANAO in October 2011 that:

> A more centralised Defence-wide approach is an integral element of the ICT Reform program being delivered as part of the SRP. This element includes creating a single enterprise architecture, standardising the Defence ICT environment and preserving system integrity and integration through more centralised technical specifications.

2.47 Defence further informed the ANAO in October 2011 that it was in the process of giving practical effect to controlling the development and commissioning of ICT initiatives by progressively centralising and restricting delegations for the purchase of software and hardware:

> CIOG's role is being promulgated by technology being controlled. The first iteration of this was the procurement of software where CIOG [*issued*] an Information Defgram (585/2011) articulating the requirements for software purchasing in Defence.

2.48 However, at the time of this audit, Defence was yet to resolve the current over-commitment of CIOG resources, placing significant pressures on both the achievement of ICT priorities and the operational day-to-day running

of Defence's ICT. In this context, Defence informed the ANAO in December 2011 that significant work has been undertaken to identify the skills needed in the future and to map out an implementation approach.

Defence ICT approval framework arrangements

2.49 Effective ICT investment approval frameworks are characterised by a defined approval process, clear identification of approval roles and a common set of criteria that aim to effectively and incisively define ICT initiatives. The ICT initiative approval process works best where there is wide understanding of the planning and approval processes among the staff that generate the proposals. This helps to ensure that proposals are available at the right time and in the right condition for a coordinated assessment by senior executive decision-makers.[68]

General ICT investments

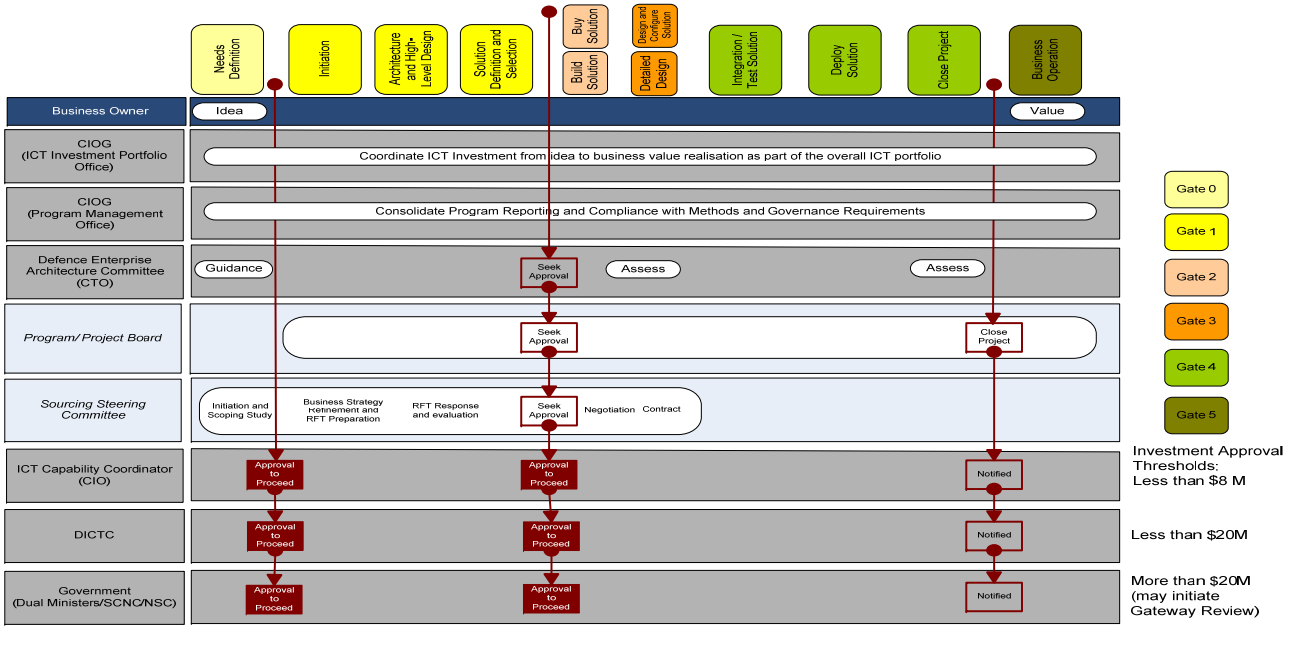
2.50 Defence has been evolving its approach to approval of ICT investments over the last few years. Currently, differing approval frameworks apply primarily depending on whether the purpose of the investment is to deliver capability to the ADF (or to the Defence organisation more broadly) and the value of the proposal.

2.51 Figure 2.3 shows the planned Defence ICT initiative approval framework as at October 2009 for investment proposals that are not primarily related to delivering capability to the ADF. Under this general approval framework, the cost of an ICT initiative determines the authority from which approval must be sought.

[68] Australian National Audit Office, *Planning and Approving Projects – An Executive Perspective*, Better Practice Guide, June 2010, p. 21.

Figure 2.3

Defence's planned ICT initiatives approval framework



Source: Department of Defence.

2.52 Many of these general ICT initiatives are within DICTC's ambit and originate primarily from the SRP, the DICT Strategy, CIOG, or from the Groups and Services.[69] Major ICT initiatives considered by DICTC have also been subject to a Defence two-pass approval process, under which the DICTC and the WFMC are required to review and approve ICT business cases prior to first and second pass.[70] The process is managed by CIOG in accordance with its role as the Coordinating Capability Manager for the DIE.

ADF Capability Development Proposals

2.53 In addition to general ICT proposals, Defence also undertakes a broad range of capital investments in support of the development of capability, including some ICT initiatives that originate as capital equipment projects designed to deliver capability for the ADF as set out in the DCP.[71] Depending on their value and purpose, specific approval processes are required by government for some of these investments.

2.54 Table 2.2 shows that the required level of approval for a proposal, whether by the Minister, the National Security Committee of Cabinet, or the full Cabinet, depends on the nature of the proposal and its likely cost.

[69] CIOG operates and maintains ICT services on behalf of the Defence business process and system owners, and can be engaged to provide new ICT business requirements. The business process and system owner customers may request changes to Defence's existing ICT capability, including requests for ICT consultancy services and the development and delivery of ICT initiatives.

[70] The ICT priorities considered by the Defence Committee are set out at paragraph 2.37, with sustainment and delivering capability as the two highest priorities. Other requirements of Groups and Services are ranked third in priority. In October 2011, Defence informed the ANAO that 'There are no Priority 3 projects on the current IPW as there was no capacity available. Minor Growth was a capped $20 million activity agreed with the October 2010 IPW to allow the SETs to manage minor business requirements from the Groups and Services.'

[71] ICT initiatives can also originate as capital facilities projects and be managed as part of the Major Capital Facilities Program (contained in the Green Book).

Table 2.2

Defence ICT initiative approval authority for capability development projects

	Type	Total cost	Initiative Approval Authority
Major project	Strategic and Complex	>$100 million	National Security Committee of Cabinet
	Strategic and Complex	>$20 million – <$100 million	Minister for Defence and the Minister for Finance and Deregulation
	Strategic and Complex	>$8 million – <$20 million	Minister for Defence
Minor Project	Minor initiative	>$8 million – <$20 million	Minister for Defence
	Minor initiative	<$8 million	Group/Service Head

Source: Department of Defence.

2.55 A two-pass approval process coordinated by the Capability Development Group applies to the largest of these projects (those classified as Major Projects and valued at more than $20 million). For Major Projects, the approval processes are complex and can extend over a long period of time. Accordingly, progressing the delivery of the ICT capability outlined in the DCP and Green Book requires CIOG to engage with a number of Defence groups and committees over an extended period. Minor capital projects, classified as projects with an overall value less than $20 million, are owned, approved and often delivered by individual Defence Services and Groups.

Whole-of-government ICT two-pass approval process

2.56 Separately, in mid 2008, a whole-of-government ICT two-pass approval process administered by the Department of Finance and Deregulation (Finance) was introduced for major Australian Government ICT initiatives in response to the *Review of the Australian Government's Use of Information and Communication Technology* (Gershon Review) with the objective of assisting government with better decision-making on ICT investments. The whole-of-government ICT two-pass process applies to ICT enabled new policy proposals

that have a total (through-life) cost estimated to be $30 million or more (including ICT costs of at least $10 million) and are high-risk in terms of cost, technical complexity, workforce capacity or schedule.

2.57 The whole-of-government ICT two-pass approval process is designed to allow government to consider whether it agrees in-principle with an initial business case proposal and if funding towards a more detailed business case will be provided. The detailed business case is then submitted for a second pass review. This staged approval process is similar to Defence's two-pass process for ADF capability development proposals, except that the whole-of-government submissions go to the Expenditure Review Committee of the Cabinet whereas Defence's submissions go to the National Security Committee of Cabinet. When the whole-of-government ICT two-pass approval process was implemented in June 2008, Defence was made exempt from these requirements.

2.58 However, in October 2009, the DICTC decided to pilot three ICT initiatives through the whole-of-government ICT two-pass approval process. The DICTC assessed that the staged two-pass approval process it was using for consideration and approval by government of major ICT initiatives in the organisation, which mirrored the process used for consideration of the Defence capability development projects included in the DCP, could not keep pace with the speed at which new technologies were introduced. This was because the lengthy approval periods to the point of second pass created unacceptable risks, and could lead to the delivery of obsolete technology.

2.59 As a result, in November 2009, the DICTC decided that all ICT initiatives *not* included in the DCP would be considered against the criteria for inclusion in the whole-of-government two-pass approval process, on the basis that it would promote the use of the accompanying administrative processes, documentation and good practices (such as the application of ICT business case tools) employed in the Finance mandated process, along with the pathways and assurance methodologies of the whole-of-government Gateway

Review Process.[72] Defence subsequently informed the ANAO in December 2011 that:

> [*the whole-of-government ICT two-pass approval process*] may also be applied to ICT projects in the DCP where agreed between the CIO and Chief Development Group via internal communications and provided the following entry criteria are met:
>
> - The project has not completed Kinnaird First Pass approval;
> - The project is delivering a capability that relates to a business process in the enabling functions of the Defence Business Model;
> - The Capability Manager is the CIO or a Business Process Owner who has agreed to the use of a 'non-Kinnaird' two-pass approval process; and
> - CIOG is the sole Acquisition Agency (indicating the solution is largely a technology implementation therefore a prerequisite for shorter delivery cycle. This would not preclude other areas from using streamlined processes if appropriate).

2.60 In practice, the DICTC considered the business cases of 24 separate ICT initiatives in its meetings from July 2008 to October 2010. Of these:

- Only 16 ICT initiatives contained a project proposal, of which eight were considered twice by the DICTC.
- Around half of the proposed ICT initiatives (44 per cent) were classified as minor projects, with costs estimates that ranged from $2.1 million to $4.7 million.
- The remaining 56 per cent of the proposed ICT initiatives were major projects with cost estimates ranging from $8.4 million to $101 million.

2.61 Table 2.3 shows an analysis of the recorded DICTC outcomes for the 16 ICT initiatives that contained project proposals.

---

[72] The Australian Government has introduced the Gateway Review Process (Gateway) to strengthen the oversight and governance of major projects and assist *Financial Management and Accountability Act 1997* (FMA Act) agencies to deliver agreed projects in accordance with the stated objectives. Gateway applies to new projects undertaken by FMA Act agencies, which require Government approval and which satisfy certain financial and risk thresholds. It involves short, intensive reviews at critical points in a project's lifecycle by a team of reviewers not associated with the project. This provides an arm's length assessment of the project against its specified objectives, and an early identification of areas requiring corrective action. Source: <http://www.finance.gov.au/gateway/review-process.html> [Accessed December 2011].

Table 2.3

Recorded DICTC outcomes for 16 ICT proposals considered from July 2008 to October 2010

Outcome	ICT project proposals considered once by DICTC	ICT project proposals considered twice by DICTC
Endorsed / Agreed	3	5
Deferred to out of session discussion	1	0
Additional work required [(a)]	3	2
No outcome recorded	1	1
Gross Total	**8**	**8**
Net Total	**16**	

Notes: (a) The type of additional work required included options or business case to be further developed, funding source to be determined and proposal to be put to WFMC for funding approval.

Source: ANAO analysis.

Defence ICT investment two-pass approval process

2.62 As part of the SRP ICT stream reform program and the DICT Strategy, Defence undertook to investigate alternatives to the Capability Development Group and Finance two-pass approval processes for Defence ICT investments, and the streamlining of its internal processes in ICT investment and capability development.

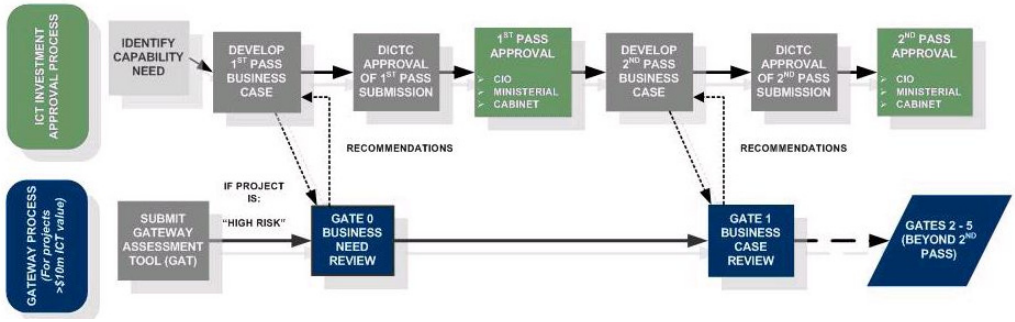
2.63 CIOG has developed a Defence ICT Investment two-pass approval process designed to condense the decision cycles for certain ICT projects, to enable CIOG to better meet the requirements of users and improve responsiveness to technology lifecycles. This two-pass approval process is managed by CIOG.

2.64 ICT-enabled projects that are subject to the ICT Investment two-pass approval process are required to apply the whole-of-government Gateway Review Process when the ICT project costs exceed $10 million and are

classified as 'high-risk'.[73] Figure 2.4 below illustrates the sequential stages of the Defence ICT Investment two-pass approval process and its interaction with the Gateway process.

Figure 2.4

The Defence ICT investment two-pass approval process and gateway



Source: Department of Defence.

2.65 Defence ICT approval processes have to date included three different two-pass processes,[74] as well as local ICT project initiation processes, leading to a complex system with multiple points of entry and diffused accountability. Defence informed the ANAO in December 2011 that:

> [*the multiple points of entry and diffused accountability*] is a reflection of the transition to a new approval process as we concurrently conduct a trial of a process that spans many months.

2.66 The outcomes to date suggest that the ICT decision-making processes are not yet mature and are still developing. Defence faces particular challenges in structuring its ICT investment approval framework, as not all Defence ICT initiatives fall within either the purview of Defence's senior ICT committee, the DICTC, and its approval processes, or within the purview of any other

[73] ICT initiatives must meet the whole-of-government two-pass process financial thresholds. The risk threshold for entry to the Gateway Review Process is high risk, as determined using the Gateway Assessment Tool (GAT). Projects that meet the financial thresholds are required to complete the GAT prior to the proposal's consideration by government to determine whether it meets the risk threshold.

Source: Department of Finance and Deregulation, Gateway Review Process, available from http://www.finance.gov.au/gateway/index.html [Accessed 24 October 2011].

[74] Depending on the project, it may have been subject to the Defence Capability two-pass approval process managed by the Capability Development Group, the Finance two-pass approval process, or the recently developed Defence ICT Investment two-pass approval process.

portfolio-level Defence decision-making body. Defence informed the ANAO in October 2011 that:

> CIOG is currently finalising the ICT two-pass process to apply in Defence in consultation with the Department of Finance and Deregulation and other stakeholders within Defence including DMO, CDG and I&S Group. This will set out in detail the steps and requirements for the Defence ICT two-pass process.
>
> In addition, CIOG has established a team to support and guide projects through the ICT two-pass process, this includes the minor ICT projects referred to in the Minister for Defence's announcement [*on the 6 May 2011 the Minister for Defence announced the introduction of a two-pass approval process for minor capital projects valued between $8 million and $20 million.*]. A number of projects are already being supported and will be the first users of the final Defence ICT two-pass process. As no project has completed the ICT two-pass process as yet, a post-implementation review has not yet been conducted.

Assessing ICT proposals

2.67 The better practice process for developing and assessing ICT initiative proposals involves two main stages: developing a project concept plan, and then a developing a comprehensive business plan. It is also better practice for an entity to define and document the common criteria that are critical when making decisions on ICT that are to be included in proposals.[75] In October 2009, the DICTC was presented with a standard business case template that was to form the blueprint for defining what an ICT investment was to deliver and assist decision-makers to determine whether the ICT capability was required, understand priorities, and select the most cost effective options to support Defence's strategic objectives.

2.68 The business case template was designed so that a non-DCP ICT proposal would set out key information such as strategic alignment, options, benefits, costs, and risks involved in a proposed ICT investment, with the aim of justifying initial approval. The template was scalable and could be used for both major and minor ICT investments, with a lesser level of detail required for minor ICT investment business cases to reflect the differences in cost, complexity and risk. The template provided a standard approach to set out

[75] Australian National Audit Office, *Planning and Approving Projects – An Executive Perspective*, Better Practice Guide, June 2010, p. 28.

cases for funding ICT investment proposals of strategic significance and demonstrate the value of investments, and supported the initial consideration and/or approval of ICT investment proposals by senior committees and decision-makers. However, the DICTC minutes do not record an outcome in respect to the Committee's consideration of whether non-DCP Defence ICT proposals should be presented using the proposed business case template.

2.69 Of the 16 proposals considered by DICTC between July 2008 and October 2010, 10 were submitted using the business case template. The majority of the business cases provided information about the proposed ICT initiatives' strategic alignment and costs. Defence informed the ANAO in October 2011 that:

> Defence is further maturing the ICT business case template to provide consistency across Defence and to align the template with the requirements being agreed with the Department of Finance and Deregulation.
>
> Defence is continuing to work on the documentation requirements for ICT projects in Defence and has dedicated a team to driving the Defence ICT two-pass process and to support ICT projects in using it.

2.70 Defence's November 2010 P3M3® maturity assessment observed that the iterative development of ICT business cases was emerging but that the quality of information recorded was inconsistent. The assessment also identified the need for a process for validating business cases in the context of the whole portfolio.[76] Without documenting the common criteria that are critical when making decisions on ICT, and analysing and scrutinising this information, Defence is limited in its ability to have informed and effective strategic ICT decision-making.

[76] PCU3ED, *P3M3® Assessment Findings: Department of Defence – Chief Information Officer Group*, Version 1.2, November 2010, p. 16.

3. ICT investment, benefits and risks

This chapter considers developments in controlling financial investment in ICT, in identifying and managing benefits, and in managing risks. It examines the treatment of these matters in the SRP, and then considers how Defence has taken up the broad framework established by the SRP to establish performance baselines to monitor progress towards performance targets.

Introduction

3.1 The SRP document, released in June 2009,[77] is the overarching plan for Defence's business management for the next ten years. Redevelopment of ICT capacity is a central component of this plan, and the achievement of SRP objectives is heavily dependent upon delivery of improved ICT capacity. Accordingly, as discussed at paragraph 1.15, significant aspects of the SRP can be characterised as a major ICT-enabled business transformation.

3.2 The SRP agenda comprises 15 reform streams.[78] The ICT reform stream is one of these and is required to deliver approximately $1.9 billion towards a total savings target across Defence of $20 billion by 2018–19. These savings will be re-invested in the Defence business, chiefly to help fund the achievement of Force 2030 as envisaged by the White Paper. In addition to delivering reforms and savings in the ICT domain, Defence's ICT initiatives were required to be responsive to the requirements of other elements of the SRP:

> [*ensuring*] that our information technology effectively supports and informs decision makers at all levels, and across all domains.[79]

3.3 The SRP established an over-arching framework for the reform process in Defence to 2018–19, including the redevelopment of Defence ICT capability. As foreshadowed in the SRP document, detailed planning for each SRP reform stream, including an implementation schedule and detailed project plan, was undertaken in the six months to December 2009 and was to include a full risk

[77] Government approved the SRP on 1 April 2009 and the public document was released on 4 June 2009.

[78] Department of Defence, *The Strategic Reform Program – Delivering Force 2030*, 2009, pp. 6-7. See Appendix 4 for a full description of the 15 reform streams.

[79] ibid., p. 5.

analysis and risk management strategies.[80] As the SRP document noted, this was a critical phase, as:

> Defence has experience of past reform efforts that have failed to deliver promised outcomes in full measure because implementation was done too quickly and without careful planning. Defence intends to get the planning phase right in order to make sure that later phases deliver what is promised.[81]

3.4 The process for implementation planning of the SRP was very complex and presented both challenges and opportunities for ICT strategic planning. The implementation process required moving from the high-level benchmarking, extrapolation analysis and senior level commitment to the broad targets established in the course of the 2008 Defence Budget Audit (DBA),[82] to a clear and implementable plan of work, verifiable components of the savings target, and a commitment at all levels within Defence to delivering the plan of work. In October 2009, about the time that Defence had originally planned to produce the SRP implementation plan, Defence advised the Government that it was still progressing development of the implementation plan, and would return to government in February 2010 with a detailed plan. The delay was attributed to the complexity and magnitude of the task of securing Defence-wide commitment to delivering the fundamental reform envisaged in the SRP document.[83]

3.5 The delay in producing an implementation plan provided more time to clearly formulate a baseline for the implementation of a program of ICT-enabled business transformation. This further planning needed to be responsive to the actions already taken at that point to implement the SRP and to address the high-level risks identified in the ongoing process of implementation planning. With regard to implementation of the SRP, the most significant factor was Defence's decision to progress with achieving the projected savings of $797 million in the 2009–10 year, by re-aligning internal budgets. CIOG was a net beneficiary of this re-alignment, receiving an additional internal allocation in 2009–10,[84] while being required to produce

---

80 Department of Defence, *The Strategic Reform Program – Delivering Force 2030*, 2009, pp. 5, 25.

81 ibid., p. 25.

82 Also known as the Pappas Review.

83 Department of Defence, *The Strategic Reform Program*, op. cit., p. 3.

84 Defence informed the ANAO in October 2011 that the only reallocations that CIOG received from elsewhere in Defence were SRP related. The total reallocation was $95.2 million in respect of Defence Information Infrastructure Security Improvement, Satellite Communications, and Infrastructure.

$49 million in savings through the ICT stream. The timing of the planned SRP investments in ICT, coming early in the process, accentuates the demands on CIOG to put in place the reforms intended to achieve the $1.9 billion projected savings for the ICT stream over the ten years of the SRP.

3.6 By October 2009, Defence had identified the high-level risk to the SRP posed by undertaking ICT initiatives to support other, critical SRP streams, while simultaneously undertaking significant remediation of Defence ICT. The March 2010 report to the Government on the portfolio-level implementation of the SRP noted that the November 2009 DICT Strategy was a 'key milestone' in assisting Defence to deliver critical ICT support to major SRP reforms, and identified a number of ICT-related issues:

- potential delays to ICT enablement posed significant strategic risks to supporting other SRP reforms;[85]
- within the ICT SRP stream, the significant complexity of consolidating enterprise hardware (for example by reducing the number of data centres from more than 200 to less than 10) and rationalising software and ICT service contracts posed risks to achieving reforms and realising the intended significant ongoing savings;
- with little flexibility left in the overall Defence budget, expediting ICT savings might be a means to respond should other SRP streams not deliver savings as planned, without significantly impacting core Defence outcomes; and
- there was a need to monitor and closely manage the risk that it would not be possible to agree and deliver on a portfolio of ICT projects across Defence.

3.7 Through the implementation planning processes for the SRP, Defence has identified the importance of managing the financial investment in ICT, including verifying the costs and savings for the ICT elements of the SRP, and identifying and managing benefits and risks. As of March 2010, CIOG had made some progress toward setting up processes and systems for developing an improved Defence-wide ICT two-pass approval process.[86]

[85] This statement is particularly significant because it highlights that, as well as risks to savings, there is a risk to achieving the SRP outcomes because significant elements of the SRP have the character of an ICT-enabled business transformation.

[86] See paragraph 2.66.

Financial investment in ICT

3.8 At the time of the appointment of Defence's first CIO in 2007, Defence had only a limited overall view of its total ICT investments and its annual expenditure on maintaining and improving its ICT infrastructure. The first stages of CIOG's 2008 survey of investments and ICT expenditure provided the initial, indicative basis of the DBA estimates of Defence ICT costs and the savings that could be made from ICT. CIOG has continued to refine its estimates, as it has pursued the identification of all Defence ICT assets and (where possible) ICT budgets and expenditure.

3.9 The DBA estimates were the cornerstone of the development of the SRP saving targets, including the ICT estimates. ICT was identified as necessary to support the broad reforms of the SRP, and so a strategy was adopted of initial investment in ICT to yield later savings, including from other SRP streams.

3.10 The DICT Strategy and the 2009 SRP document set out total annual ICT expenditure in 2008–09 of $1.2 billion, including both investment initiatives and business-as-usual. A March 2009 DICTC agendum paper forecast Defence ICT expenditure of $1.316 billion in 2008–09. According to the Defence White Paper ICT Companion Review (prepared in September 2008), 'Defence costs an estimated $1.678 billion in ICT across the portfolio annually'. Defence informed the ANAO that this figure included in the Defence White Paper ICT Companion Review incorrectly included approximately $400 million in depreciation.[87]

3.11 Defence commissioned a consultant to prepare an ICT Baseline Report outlining Defence's enterprise-wide ICT expenditure, which was completed in January 2010 after the first version in December 2009 was incomplete due to missing information from some Groups. The January 2010 ICT Baseline Report estimates annual personnel costs for ICT at approximately $277 million, whereas the Defence ICT Reform Program Design Manual[88] (PDM) (delivered in December 2009 by the same consultant) cites personnel costs of $153 million per annum. Defence informed the ANAO in December 2011 that:

> The Defence ICT Costing Baseline activity is in its third year and this provides Groups and Services with a view of their ICT spends. The financial

[87] The 2008 DBA stated that 'the total projected spend [for 2008–09] is $917 million' (excluding personnel costs). Source: McKinsey and Company, *2008 Audit of the Defence Budget,* April 2009, p. 194.

[88] The PDM sets out the implementation plan for the DICT Strategy.

> information populating the Defence ICT Costing Baseline has and continues to be progressively validated as needed against the Defence financial systems (ROMAN and BORIS) records. This strategy is to ensure that Group and Service Heads understand and own the ICT activities that are performed within their own space.
>
> Defence recognises that the information has not been sufficient to date and CIOG is working to improve this.

3.12 The ICT Baseline Report calculated a Defence-wide ICT expenditure of approximately $1.282 billion for 2008–09. This is further discussed in paragraph 3.20.[89] None of these estimates includes the cost of the ICT components of deployable military equipment.

Cost savings

3.13 The 2009 DICT Strategy sets out ICT reform investments of approximately $940 million over the four years from 2009–10 to 2013–14, which are expected to assist the delivery of $1.9 billion in savings over the decade and around $250 million per annum thereafter.[90] The 2009 SRP document indicates an investment of $668 million over the same four years ($708 million over the decade), with net savings over the decade of $1.240 billion.[91] Defence informed the ANAO that these savings targets were derived from the DBA which, in turn, reported that:

> [*Working*] with CIOG, we developed an approximate bottom-up sizing of the efficiency opportunity, which we then verified against a top-down opportunity sizing based on our experience working with other clients on similar ICT reform plans.[92]

3.14 The components of the overall savings target included in the SRP, including the ICT component, were not costed in detail:

---

89 As discussed in Chapter 2, Defence is yet to achieve an enterprise-wide agreed basis for estimating and reporting ICT budgets and expenditure. For instance, the September 2008 Defence White Paper ICT Companion Review cited DMO's annual expenditure on ICT of $329 million. CIOG informed the ANAO in July 2010 that the estimated total annual ICT expenditure by DMO is approximately $171 million, but this figure has not been agreed by DMO and does not include ICT expenditure as part of capital equipment projects managed by DMO.

90 Department of Defence, *Defence Information and Communications Technology Strategy 2009*, p. 8.

91 Department of Defence, *The Strategic Reform Program – Delivering Force 2030*, 2009, p. 27 (Attachment A).

92 Pappas, G. *2008 Audit of the Defence Budget*, Department of Defence, 2009, p. 193.

> This [*savings*] target is underpinned in the main by high-level benchmarking and extrapolation analysis undertaken by the [*Defence Budget Audit*]. The Government has agreed to allow some flexibility in the way Defence achieves this target. As the detailed planning and implementation of the Strategic Reform Program proceeds over the next six months more savings will be found in some areas and less in others. What won't change is Defence's commitment to meet the overall savings target. Indeed, wherever possible Defence will be striving to overachieve in each savings stream.[93]

3.15 However, the estimation technique used in support of the DBA estimates is proprietary: neither the data input nor the estimation technique is visible to Defence. Defence informed the ANAO that the savings opportunity identified by consultants and adopted in the 2009 SRP document had been calculated by the DBA using a baseline from a 2007 consultant's analysis of Defence's ICT spending. Defence further informed the ANAO in December 2011 that:

> The Defence Budget Audit (DBA) identified opportunities for reform rather than being a precise calibration of Defence's cost base. These opportunities were then explored in detail during the detailed planning phase [*of the SRP*]. The diagnostics and planning phase established the cost reduction targets. These targets were then removed from forward budgets to create an incentive to reform. DBA also identified the need for remediation of Defence's backbone including ICT and so an appropriate investment and saving strategy was developed around the ICT Stream.

3.16 In this circumstance, there is little evidence available to validate the process to develop the SRP ICT savings target or assess the likelihood of these savings being realised, particularly given that:

- the DBA's 'top-down opportunity sizing' was 'based on [*the consultant's*] experience working with other clients on similar ICT reform plans', though these are not identified, and Defence's situation would appear to be unique; and
- as shown at paragraph 3.10, estimates of Defence's spending on ICT have varied widely and cost savings identification is unlikely to be robust without an accurate view of how much is currently being spent.

[93] Department of Defence, *The Strategic Reform Program – Delivering Force 2030*, 2009, p. 9.

Establishing a baseline for the cost of Defence ICT

3.17 An important element of cash benefits realisation from investment is to firstly understand the ICT cost base against which benefits will be measured. As discussed in paragraph 3.10, Defence has calculated and reported in various documents varying amounts as its total per annum cost of ICT. CIOG advised in 2010 that '[we] tend to use a figure of approximately $1.3 billion when discussing the total [Defence] ICT cost'. As previously noted, this excludes the costs of ICT components on deployable military equipment.

3.18 To assist in understanding the costs of its current ICT infrastructure, Defence engaged a consultant to develop an ICT Baseline Report, detailing the ICT expenditure across all areas of Defence for 2008–09. The primary function of Defence's ICT Baseline Report is to support the realisation of benefits from the SRP ICT Stream. This is intended to be achieved through establishing an ICT cost-base against which the cash benefits realisation, portfolio management and risk, and interdependency management methodologies are measured and tracked. Secondary objectives of the ICT Baseline Report are to increase the transparency of Defence-wide ICT expenditure and allow benchmarking against other Australian Government agencies.

3.19 In developing the cost-base, all Defence Groups and Services were required to provide data on their ICT expenditure, personnel, assets, resources and activities at an agreed point in time. Defence informed the ANAO that the majority of the Groups provided ICT expenditure data, with the exception of the DMO and the People, Strategies and Policy (PSP) Group. Accordingly, these two groups were not included in the overall expenditure figure along with the I&S Group, due to the classified nature of its data.

3.20 The ICT Baseline Report estimates total annual ICT expenditure across Defence at $982 million in 2008–09, but this does not include expenditure by the DMO, PSP Group or I&S Group. The consultants estimated the combined DMO, PSP Group and I&S Group ICT expenditure to total $300 million, thereby bringing the total estimated Defence ICT expenditure for 2008–09 to $1.282 billion. In October 2011, Defence informed the ANAO that

> In the second year of whole-of-Defence ICT costing activity, data was received by CIOG from both the DMO and PSP Group. As there are now two years of data available, the Defence ICT costing model has been, and will continue to be refined into the future.
>
> Defence recognises that there has been a lack of consistency and agreement at Department level for ICT costings, notably about attribution of costs, people

and services. Disagreements are being resolved across Defence as individual issues are addressed.

3.21 Defence informed the ANAO that the Defence ICT expenditure estimate for 2010–11 is $1.241 billion.

Benefits planning and management

3.22 Simply investing in and implementing ICT initiatives does not by itself guarantee the generation of business value (or benefits). Experience has demonstrated that ICT investments that are actively planned and managed to deliver specified benefits are most likely to produce the expected business value. In the context of Defence's integrated ICT reforms, benefits realisation is the process that ensures the desired ICT outcomes are clearly defined, are measurable and are realised through a structured approach. Having in place a framework that maps expected ICT benefits to specific quantifiable metrics, and an ongoing process to track and monitor the expected benefits, also provides for an opportunity for intervention if benefits are not being achieved as planned.

3.23 Defence's planning documentation for the ICT stream of the SRP outlines two types of benefits that are anticipated to be realised through its ICT reform program: cash and non-cash. Cash benefits are defined as delivering business value through the reduction in operating expenses, for example personnel and sustainment costs, and reduced capital expenditure. Non-cash benefits are defined as delivering business value through improvements to ICT governance, capability and service delivery, and improvements to staff skills and engagement. Non-cash benefits were linked to the strategic imperatives outlined in the DICT Strategy.

3.24 Defence has developed Key Performance Indicators (KPIs) to measure the cash and non-cash benefits derived from the implementation of ICT initiatives. Defence informed the ANAO in October 2011 that:

> Cash benefits for the [SRP] ICT Reform Stream are being measured and monitored. There is an agreed activity to mature the non-cash benefits by the end of 2011–12. Business-as-usual services are currently being measured through the CIOG Performance report.

SRP ICT stream performance indicators and monitoring mechanisms

3.25 Table 3.1 outlines the four planned KPIs for the SRP ICT stream articulated in the SRP Integrated Performance Management Model (IPMM).[94] As shown, the SRP ICT stream indicators are all quantitative measures, covering both cash and non-cash benefits. Defence informed the ANAO in December 2011 that:

> The indicators result in a percentage that is then rated as green (>80%), amber (60–80%) or red (<60%) based on performance report thresholds and used across all streams. The baselines/baseline standards are built in to the indicators (generally measured against the baseline year performance). In the case of financial indicators the measure is either a red (you didn't live within your means) or green (you did).

[94] The IPMM measures achievement of SRP objectives, overall program effectiveness and the SRP's impact on the organisation.

Table 3.1

Key indicators tracking the SRP ICT stream performance

ICT Indicator	Objective	Calculation
Percentage of reform activities rolled out on schedule	To determine whether planned reform activities are being implemented on schedule as outlined in the stream implementation plan	Number of reform activities on schedule --- Total number of reform activities
Percentage of reduced budgets living within their means	To determine whether ICT savings are being achieved from the areas expected	Number of Group sub-category budgets where actual expenditure is within budget --- Total number of Group sub-category budgets
Percentage of ICT performance metrics meeting target performance levels	To measure whether business is continuing at agreed service levels	Number of Key Result Areas meeting or exceeding agreed service levels --- Total number of Key Result Areas
Percentage of ICT non-cash benefit targets achieved on schedule	To measure whether organisational ICT capability development objectives are being achieved as planned	Number of ICT non-cash benefit targets achieved on schedule --- Total number of ICT non-cash benefit targets

Source: Adapted from Department of Defence documentation.

3.26 The SRP performance indicators are reported to Government biannually. Table 3.2 shows the relevant reports against KPIs for the period January to June 2011.

Table 3.2

January to June 2011 SRP ICT stream performance report

ICT Indicator	Objective	Reported result
Percentage of reform activities rolled out on schedule	To determine whether planned reform activities are being implemented on schedule as outlined in the stream implementation plan	86%[(a)]
Percentage of reduced budgets living within their means	To determine whether ICT savings are being achieved from the areas expected	29%
Percentage of ICT performance metrics meeting target performance levels	To measure whether business is continuing at current levels	68%
Has Defence lived within the total ICT budget?	To determine whether ICT cost reductions are being achieved from the areas expected	No
Overall ICT SRP Performance Index Score = 56%		

Notes: (a) Defence's target for this indicator is 80% or greater.

Source: Department of Defence.

3.27 Defence informed that ANAO in October 2011 that the development of KPIs for non-cash benefits (shown in the last row of Table 3.1) would proceed as suitable data becomes available:

> 'Percentage of ICT non-cash benefit targets achieved on schedule' – has never been measured in any performance report as Defence currently does not have data of suitable veracity to warrant inclusion at this stage but Defence would like to include such a measure in future reports, once appropriate data is available.

3.28 The SRP biannual report to government includes commentary reporting against the state of capability and improvement analysis of any benefits or issues. The January to June 2011 ICT Stream report identified that the low score was due to CIOG's 2010–11 overspending their budget as a result of investing in the replacement of end-of-life Data Centre infrastructure, the acceleration of projects in the IPW to satisfy customer demands, and the advanced payment of software licence renewals to take advantage of early

payment discounts. Efficiencies were also reported to have been realised through various activities.[95]

3.29 The ICT Stream faced challenges in delivering agreed benefits on schedule. The SRP biannual report for January to June 2011 identified the risks to delivering SRP ICT reform benefits as:

- resource demand exceeding supply; and
- market availability of specific skill sets.

Risk management

3.30 The ICT Portfolio Management Office (ICTPMO) is assigned the responsibility for identifying, collecting, classifying, assessing and tracking issues and risks to the ICT reform program. Risks are rated using a standard five-by-five matrix of consequences and likelihood.

3.31 Issues and risks shared by multiple projects, requiring program-level management, are to be recorded in an Issues Register and a Risk Register. These registers are maintained by the Directorate of Group Governance and Reporting and are provided to the CIOG Corporate Governance Committee on a monthly basis for review.

3.32 The Issues and Risk Registers are intended to be the basis for reporting and, if necessary, escalating matters for consideration by the DICTC, the Defence Audit and Risk Committee or the Strategic Reform and Governance Executive. However, while the PDM sets out a process for escalation of issues, there is no explicit corresponding process set out for the escalation of risks.

3.33 While the PDM mandates the development and maintenance of issues and risk registers which cover ICT risks across Defence, it does not indicate when the central risk and issues registers will be implemented, the relevant processes to be promulgated by the PMO, or when they will be promulgated. The PDM would also benefit from the inclusion of information on:

- the current state of risk and issues management in CIOG, and the significant gaps in these that limit its ability to manage the program;

[95] Department of Defence, *Strategic Reform Program Performance Report for the period January–June 2011*, p.12-13. The various activities include: reduced software and support costs ($20.3 million); reduced hardware costs ($10 million) improved fixed and mobile telephone contracts ($22 million); reductions through the Sustainment Efficiency program ($10.3 million); and improved ICT support contracts through the consolidation of existing contracts ($24 million).

- how and when these gaps will be filled; and
- who will be accountable for the changes.

3.34 Defence informed the ANAO in October 2011 that:

> ICT Reform risks are considered regularly at the CIOG Executive level and there is an escalation path through to Senior Defence Committees including the Defence Audit and Risk Committee (DARC), the DICTC and the ICT Reform Stream Governance Committee.

Implementation of risk management

3.35 The ANAO examined the Defence ICT Reform Program-Level Risk Register (Risk Register) and the Defence ICT Reform Program-Level Issues Register (Issues Register). The Risk Register listed a total of 22 risks at the time of the audit, while the Issues Register listed three issues.

3.36 As part of CIOG's risk and issues management process, the PDM states that the ICT Reform Office identifies risks and issues that are 'shared by multiple projects which require program level management'. According to the PDM, these multiple-project risks and issues then populate the Issues and Risk Registers, along with risks and issues from stakeholder questions and the ICT Reform Office's own analysis. These issues and risks have been incorporated into the Issues and Risk Registers.

3.37 The ANAO reviewed the Project Status Reports and found that deficiency in workforce resources was the key risk and issue common to multiple projects. The ICT Reform Program has been subject to employee resource constraints since its inception. The significant number of ICT reform projects being undertaken simultaneously has resulted in the oversubscription of full-time employees, primarily from CIOG. The significance of the risks presented by the workforce shortage is such that the achievement of the ICT Reform Program, and indeed the broader SRP, may be adversely impacted. Defence advised the ANAO in October 2011 that:

> Skills and capabilities needs in CIOG are being addressed through a number of approaches including the increased allocation of staff to projects (from 250 to 380). There has been no material impact on business-as-usual.
>
> The CIOG Strategic Workforce Review has identified the skills required and set out a plan to transition to the new workforce structure.
>
> In addition, establishment of AMSPA [*Applications Managed Service Partnership Arrangement*] and the approach to sourcing through the bundles is also addressing the workforce issues the ANAO has identified.

3.38 CIOG's workforce pressures are further discussed in Chapter 4.

Interdependencies

3.39 A key risk domain is that of interdependencies between projects. The 2009 SRP document outlines the developments in ICT capability that are planned to occur by 2018–19 in broad terms. These developments have Defence-wide components and implications and are significantly inter-connected. They represent a significant challenge for ICT strategic planning.

3.40 Table 3.3 summarises all SRP initiatives by objective and SRP Stream, identifying whether they explicitly include an ICT initiative (Category A) or whether they implicitly rely on other ICT initiatives identified in the IPW (Category B). Table 3.3 shows that ICT initiatives are a very substantial component supporting the SRP, cutting across most SRP Streams, consistent with significant components of the SRP having the character of ICT-enabled business transformation. Of concern is that the SRP proposals and plans do not explicitly identify or consider the implication and risks resulting from the interdependencies between these various initiatives. Failure to identify interdependencies (and so the portfolio critical path) greatly increases the chance of initiative slippages and in turn puts the timely achievement of SRP outcomes at risk.

3.41 The multiple ICT reform agendas underway in Defence present particular complexity in the organisation's ICT portfolio. ICT initiatives can not be considered in isolation as the outcome or processes from one ICT initiative are often necessary for the processes or outcome of another ICT initiative. The ICT interdependencies of the SRP are particularly important to manage, given the integral role ICT plays in enabling the other reform streams. As the SRP Streams are individually managed and governed, there is a risk that a stream will depend on ICT to achieve the required savings, or other critical reform outcomes, without the full knowledge of CIOG. This may result in there being greater demand than has been catered for, or poor synchronisation between when the ICT capability is scheduled to be developed and when the benefits are expected to be delivered by the other SRP Streams.

Table 3.3

SRP initiatives with ICT involvement

SRP Stream related category	Initiative	Category A or B
Improved accountability		
Not specified	Improved management information systems	A
Not specified	Enhanced business planning and enterprise level risk management functions	B
Not specified	Continual improvement of advice to the Government and Ministers	B
Not specified	New output-focused budget model	B
Improved planning		
Capability development	Improved cost forecasting for major acquisitions	B
Capability development	Improved risk planning for projects in the Defence Capability Plan	B
Procurement and sustainment	Baseline scope, cost, risk and schedule for major acquisitions	B
Preparedness and personnel operating costs	Cost/benefit model to support decisions optimising preparedness	B
Preparedness and personnel operating costs	Refining the preparedness management system	A
Preparedness and personnel operating costs	Improvements to Defence financial and human resource management systems	A
Enhanced productivity		
Smart sustainment	Improved inventory management	B
Storage and Distribution (logistics) Reform	Improved logistics planning, management and execution systems, including Automated Identification Technology	A
Storage and Distribution (logistics) Reform	Improved land materiel maintenance system	B
Non-equipment procurement	Procurement and Contracting Centre of Excellence technology	A
Non-equipment procurement	Greater use of e-business and use of automated procurement processes	A
Information and Communications Technology	Single DIE network	A

SRP Stream related category	Initiative	Category A or B
Information and Communications Technology	Refresh ICT infrastructure	A
Information and Communications Technology	Data centre rationalisation	A
Information and Communications Technology	Improved ICT management	A
Intelligence	Restructuring ICT capabilities of the three Defence intelligence agencies	A
Science and Technology	ICT enablement of revised science and technology business processes	B
Reserves	Reserves skills database	A
Defence Estate	Rationalisation of the Defence estate, ICT infrastructure and services	B
Defence Estate	ICT enablement of improved estate management business processes	B

Source: ANAO analysis of the SRP.

Notes: **Category A** initiatives are those identified by Defence in the SRP as having an ICT component.

Category B initiatives are those that ANAO assesses as requiring ICT development, but not specifically identified by Defence.

The table classifies initiatives by 'SRP Stream related category' rather than by 'SRP Stream' because the headings under which the initiatives appear in the text of the 2009 SRP document do not correspond exactly with the SRP Streams identified in the SRP.

3.42 Defence's implementation planning for the SRP recognises the successful delivery of ICT systems as a key dependency that will support the implementation of the reforms and generation of the associated savings. Identifying, mapping and resolving how the SRP interdependencies are managed is the role of the Strategic Reform and Governance Executive. At the SRP Stream and Group level, Senior Executives are responsible for managing interdependencies. Where significant decisions around cross-portfolio reprioritisation are needed, they are escalated to the Defence Committee (DC).[96]

[96] The Defence Committee (DC) is the pre-eminent committee in Defence. Its role is to make decisions that assist in achieving the results specified in the Ministerial Directive to the Secretary and the Chief of the Defence Force. It comprises the Secretary and CDF.

3.43 A first version of a SRP interdependencies map was presented to the DC in September 2010, some 15 months after the public announcement of the SRP. The map provided a strategic overview of potential or emergent risks that were arising due to significant interdependency issues that needed to be resolved across the SRP enablers of Estate, ICT, and Policy and Procedure. Of the 37 interdependency issues identified, 49 per cent (18) were ICT interdependency issues, with three of the ICT interdependency issues relating to five SRP Streams and one ICT interdependency issue relating to two SRP Streams. The map identified 19 areas of the SRP that could be impacted on, and the consequent materiality if the interdependencies were not effectively managed. At that time, ICT interdependency issues were linked to 10 (53 per cent) of these SRP areas, putting the realisation of an estimated $1.7 billion of the SRP savings at risk.

3.44 Defence recognised that the SRP interdependencies map would change as new interdependencies were identified and the relative significance of known interdependencies shifted as implementation proceeded. The DC agreed to consider SRP interdependencies on a bi-monthly basis. However, a February 2011 version of the interdependencies map shows that, since September 2010, there has been minimal further development of the mapping of ICT interdependences and the potential risks to the SRP savings.

3.45 The February 2011 updated interdependencies map introduced an interdependency status report, with options to report individual interdependencies as 'being managed at the Stream level and does not require DC discussion', 'problematic and would benefit from DC discussion', and 'requires DC intervention'. The majority of the interdependencies were reported as being managed effectively at the stream level; with three of the interdependency issues reported as problematic (two of these were ICT interdependencies).

3.46 The implementation status of interdependencies is also reported in the three categories of: on track; some slippage to the implementation schedule; or implementation schedule materially affected. Around 50 per cent (eight) of the ICT interdependencies were reported to have some slippage to the implementation schedule, with the implementation of the remaining ICT interdependencies (nine) reported as being on track.

3.47 The ICT interdependency issues have been reported as presenting risks to the SRP. These risks are relevant to Defence's ICT environment and broader ICT work program outside of the SRP. Failure to identify interdependencies

(and the portfolio critical path) greatly increases the chance of initiative slippages, and in turn puts the achievement of ICT priorities at risk. The process of identifying, mapping and sequencing ICT initiatives is a key part of the prioritisation process. Even given the measures currently being undertaken to alleviate resource shortages, it is not clear that the initiatives on Defence's ICT work program will make the progress expected unless they are appropriately staged. However, neither the PDM nor the DICT Strategy included a discussion of specific risks at the portfolio or program level.[97] In this respect, Defence's PDM provides a useful format for recording and illustrating interdependencies. In practice, CIOG has relied on individual project managers to identify interdependencies. Defence informed the ANAO in December 2011 that:

> Maturity of the ICT interdependencies from other SRP streams has improved significantly this year with greater partnering with the business owners of systems such as Human Resources, Finance, Estate Management, Preparedness, Security and Logistics.
>
> The nature of specific interdependencies will become clearer as the Streams are able to articulate in more detail, with CIOG's help, their actual ICT requirements.

3.48 The February 2011 Defence ICT Strategic Assurance Review reported that interviewed stakeholders cited a lack of a portfolio-wide view of interdependencies as a concern. Consultants were engaged in 2011 to progress the understanding of the top 15 ICT initiatives of Defence's program of work, including interdependencies.

3.49 At the time of this audit, the 24 SRP initiatives outlined in Table 3.3 had yet to report any interdependencies, suggesting that a much more robust and systematic top-down analysis is required. There is also little evidence in the PDM that attention has been paid to the appropriate sequencing of projects with regard to interdependencies and resource contention.

3.50 In view of the crucial importance of ICT capacity redevelopment to the success of the SRP, the analysis of how ICT is to support implementation of other streams of the SRP would have benefitted from early attention. In particular, the linkages between the ICT and other streams of the SRP needed

[97] With the exception of workforce risk, identified in the DICT Strategy. Defence informed the ANAO that project-level risks are managed through individual projects.

to be addressed, including by specifically describing the interdependencies between them. Interdependency mapping is a key discipline in a change program of this magnitude, and its treatment in the PDM indicates that much work remains to be done in this area.

4. Chief Information Officer Group management maturity

This chapter examines the program-level management maturity of the Chief Information Officer Group according to the internationally accepted P3M3® model, and the role of the Group as a key program office supporting a range of important ICT investments in the Defence portfolio.

Introduction

4.1 Management maturity models, notably the Portfolio, Programme and Project Management Maturity Model (P3M3®) of the United Kingdom Office of Government Commerce (OGC),[98] are now being widely applied to help drive up standards and capability in public sector management. Following the Gershon Review,[99] P3M3® was mandated by the Department of Finance and Deregulation (Finance) for assessing the maturity of Australian Government agencies' processes for managing their ICT portfolios.

4.2 In its most recent form, the P3M3® assessment regime is designed to apply to any organisation and any management process. The methodology has evolved significantly from its origins in assessing the management of ICT, and now is being applied more broadly to measure the maturity of organisations' management of their investments at the portfolio, program and project levels, as shown in Figure 4.1. The P3M3® portfolio, program and project levels encompass (respectively) an organisation as a whole, a set of related projects within an organisation, and individual projects, as follows:

- Portfolio management: managing the totality of an organisation's investment in the changes required to achieve its strategic objectives. Responsibility for portfolio management lies at a very high level within the organisation and it is intended to enable the most effective balance of organisational change and business-as-usual;

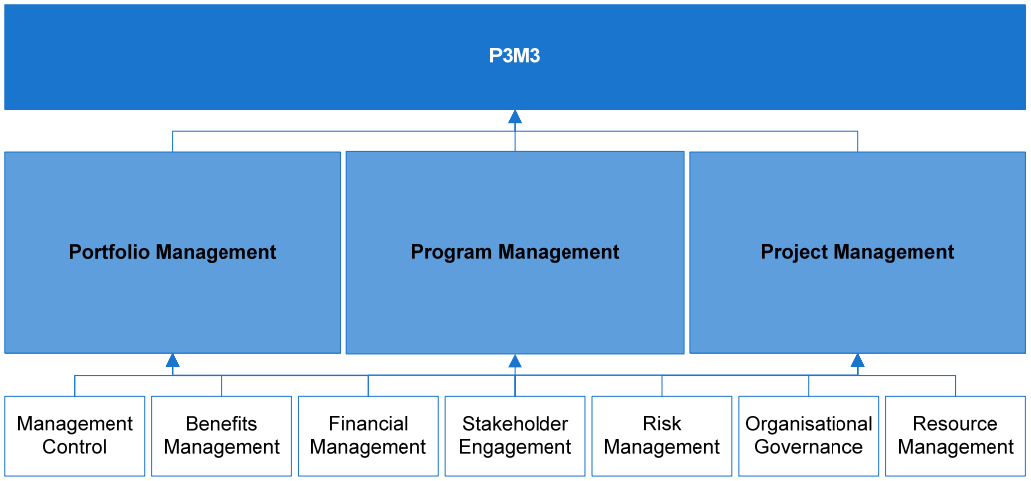
[98] P3M3® is owned by OGC.

[99] Sir Peter Gershon, *Review of the Australian Government's Use of Information and Communication Technology*, Commonwealth of Australia, 2008, Recommendation 2, p. 66.

- Program management: planning, organising, directing and controlling of a group of related projects, often with the aim of delivering change and/or improvements to an organisation's performance; and
- Project Management: guiding a project through a visible set of activities, from controlled start-up, through delivery, to controlled closure, and review. [100]

Figure 4.1

P3M3® structure



Source: Adapted from the UK Government Office of Government Commerce. [101]

4.3 At each level, management maturity is gauged with reference to seven Process Perspectives: Management Control; Benefits Management; Financial Management; Stakeholder Engagement; Risk Management; Organisational Governance; and Resource Management. The overall management maturity rating assigned to a level is the rating of the *least* mature Process Perspective within that level.

4.4 Maturity ratings range from one, which corresponds to management awareness that processes exist to bring goals into reality (though the processes may not be complete or it may not be documented), through to higher levels of

[100] OGC, *P3M3® – Portfolio Model,* 2010, Version 2.1, p. 2.

[101] OGC, *P3M3® – Introduction and Guide to P3M3®,* 2010, Version 2.1, p. 7.

maturity up to a rating of five, at which processes are optimised.[102] Under P3M3®, each of the portfolio, program and project levels is rated independently and the organisation can use the results to identify:

> …a process improvement pathway along which they may choose to travel. This journey should be seen as a long-term strategic commitment rather than a quick fix for immediate tactical problems.[103]

4.5 In this respect, the audit focus was on the efforts Defence is making to establish portfolio and program level management of its ICT, consistent with the re-shaping of business practices being effected through the SRP. Taking into account the experiences of other organisations that have embarked on ICT-enabled business transformation, including sources of better practice guidance, the ANAO formulated steps along the developmental pathway of portfolio and program management against which Defence's progress can be gauged. As outlined in Table 4.1, these steps acknowledge the importance of establishing governance structures and processes as a necessary pre-cursor to defining, promulgating and putting them into practice within the organisation.

[102] The five maturity ratings of P3M3® are: Level 1: awareness of process; Level 2: repeatable process; Level 3: defined process; Level 4: managed process; and Level 5: optimised process. Detailed descriptions are provided in Appendix 3.

[103] UK Office of Government Commerce, 2010, *P3M3® – Introduction and Guide to P3M3®,* Version 2.1, p. 13.

Table 4.1

Development pathway for portfolio and program management

Process	Portfolio level	Program level
Establish	Commitment and engagement of strategic level management Governance structures and processes	Allocation of responsibilities to managers Risks related to the division of responsibilities
Define	Benefits to be achieved Timeframe Amount of Investment Portfolio level risks and issues	Organisational capability that will produce benefits Structure of projects that will produce capability efficiently and effectively (including mapping of interdependencies) Program level risks and issues
Monitor	Achievement of benefits Investor satisfaction Management of portfolio level risks and issues	Delivery of capability Performance of individual projects Program level risks and issues
Review	Against investor expectations	Impact of project changes on capability

Source: ANAO analysis of better practice including P3M3®, Program Management Body of Knowledge, United Kingdom National Audit Office Guidance on achieving ICT-enabled business transformation, Queensland Government and Canadian Government IT Governance standards.

CIOG as a program manager for Defence

4.6 As discussed in Chapters 1 and 2, much of Defence's current portfolio of investment in change is focused on the SRP, in support of achieving the objectives of the 2009 Defence White Paper. Each reform stream of the SRP portfolio, including the SRP ICT Stream, can be viewed as an investment program comprising significant projects, among which are major ICT projects.

4.7 The SRP ICT Stream is unique in that it is solely comprised of major ICT projects. Functionally, when viewed from the perspective of the Defence portfolio as a whole, CIOG is directly or indirectly involved in the delivery of

six major programs of ICT investment with an estimated total expenditure of $1.6 billion over the period 2010–11 to 2013–14.[104]

4.8 CIOG's program-level activities stem from the centralised governance and management of the ICT reform agenda—including managing resources, providing organisation-wide communication, undertaking program-level risk management, and coordinating activities across all ICT projects—all of which are geared toward ensuring that the intended outcomes of the SRP and DICT Strategy are achieved and are aligned with Defence's overall strategic vision. In the context of the SRP as ICT-enabled business transformation, CIOG is a good fit with the P3M3® program model, in which a program is a:

> …flexible organisation created to coordinate, direct and oversee the implementation of a set of related projects and activities in order to deliver outcomes and benefits related to the organisation's strategic objectives. … Programs provide an umbrella under which projects can be coordinated, and the program integrates the projects so that it can deliver an outcome greater than the sum of its parts.[105]

4.9 The November 2010 independent portfolio-level P3M3® assessment of CIOG can therefore be taken as a reasonable guide to the maturity of CIOG as a program manager with significant and diverse responsibilities for ICT within the Defence portfolio, particularly the SRP portfolio of investment. This perspective accords with Defence's intention to move from separate Services and Groups each looking after their own ICT, to CIOG taking on the role of coordinating capability manager for all Defence ICT.[106]

P3M3® assessment of CIOG

4.10 In November 2010, CIOG received the results of a P3M3® assessment undertaken by an independent, registered consultant.[107] Defence was rated as

---

[104] The six major ICT programs of investment are: Data Centre Consolidation ($417m); Terrestrial Communications Bundle ($156m); Next Generation Desktop ($417m); Distributed Computing Services ($151m); Infrastructure Remediation ($388m); and Software Licence Rationalisation ($91m).

[105] UK Office of Government Commerce, 2010, *P3M3® – Programme Model,* Version 2.1. p. 2.

[106] See CIOG, *ICT Operating model,* 2010, and CIOG, *The New Culture,* 2011.

[107] Program Planning Professionals Pty Ltd (PCU3ED), *P3M3® Assessment Findings, Department of Defence – Chief Information Officer Group*, November 2010. The assessment responded to Finance's requirement that agencies subject to the *Financial Management and Accountability Act 1997* (FMA Act), including the Department of Defence, undergo a P3M3® assessment of their management of ICT. The assessment measured CIOG's capability to deliver their ICT investments and to plan capability improvements.

having no standard portfolio processes, as all processes were not fully defined, documented, widely understood and consistently applied through an organisation-wide approach to delivery. The assessment did, however, identify areas of good governance in portfolio and project management, as well as areas in which improvements could be made. The assessed maturity rankings were on a par with those of most other organisations that have been subject to P3M3® assessments,[108] and were as follows:

- **Project Management – Two: Repeatable Process.** This ranking indicates that 'each project is run with its own processes and procedures to a minimum standard; however there is limited consistency or coordination between projects'.
- **Program Management – One: Awareness of Process.** This indicates that CIOG 'does not consistently recognise programs as running differently from projects, and there is no standard Program Management process'.
- **Portfolio Management – Two: Repeatable Process.** This indicates that 'an executive board recognises programs and projects as organisational investments, however there are no standard portfolio processes, and limited consistency and coordination across programs and projects'.[109]

4.11 The maturity levels assigned to the process perspectives underlying CIOG's Portfolio Management were all ranked at two. This accorded with the results of CIOG's P3M3® self-assessment, and was comparable to the P3M3® maturities of other Australian Government agencies assessed at that time.[110]

4.12 The independent assessor noted CIOG's recent achievements in putting in place portfolio management processes and recommended that:

> As many of these portfolio management processes are newly implemented and still undergoing refinement, the [*CIOG*] Portfolio Management Office is newly established in its current form, it is recommended that [*CIOG*] focuses

[108] The highest level of maturity so far awarded to any Australian Government organisation is three, corresponding to an organisation with defined processes for achieving organisational purposes: see UK Office of Government Commerce, 2010, *P3M3® – Introduction and Guide to P3M3*, p.13.

[109] PCU3ED, *P3M3® Assessment Findings: Department of Defence – Chief Information Officer Group,* Version 1.2, November 2010, pp. 5, 6.

[110] See, for instance, Tanner James, *P3M3® Assessment Report: Australian Government: Department of Families, Housing, Community Services and Indigenous Affairs*, 13 August 2010, pp. 9–14.

on consolidating its current [*maturity ranking*] by embedding these processes rather than introducing any new disciplines.

4.13 Defence informed the ANAO in December 2011 that:

> Since the P3M3® assessment in November 2010, CIOG has made a concerted effort to improve its maturity recognising its capability needs to be at a level that balances the inherent risk in delivering its reform program. Targeted capability improvements have focused in on governance, accountability, benefits management, resource management and scheduling.

P3M3® process perspective maturity assessments

4.14 P3M3® identifies key characteristics of good program-level governance as: clear and visible leadership to maintain the strategic alignment of programs; demonstrable reporting lines to the Executive level; Executive approval of all programs; active Executive engagement with programs and related business change activities; and active management of interdependencies between programs.[111]

4.15 In the following sections of this chapter, CIOG's progress toward achieving good program-level governance is examined with reference to each of the seven P3M3® process perspectives (see paragraph 4.3), updated with observations from recent assessments of CIOG's ICT Reform Program. A more detailed assessment of CIOG's capabilities and challenges emerges, as does a range of important issues for consideration at the portfolio management level, including for the SRP.

Management control

4.16 Program-level management control involves the life cycle management and maintenance of a program. It is characterised by internal organisational factors such as clear evidence of leadership, direction and regular review processes. Any issues identified are dealt with through a structured process, allowing necessary program adjustments to be made to ensure alignment with organisational strategies. Effective management control is critical to the success of a program.

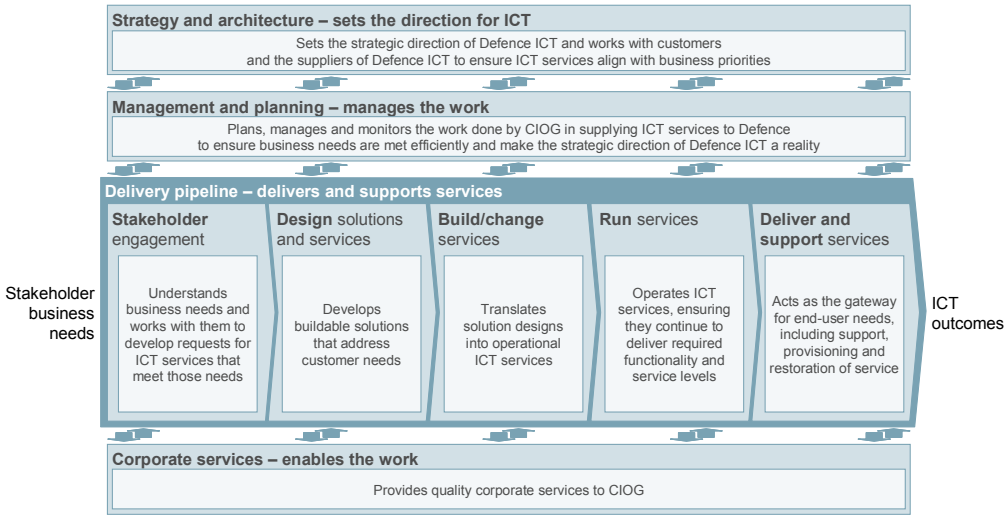
4.17 In late 2010, CIOG promulgated an Internal Operating Model outlining its approach to the overall management of Defence's ICT services, including

[111] UK Office of Government Commerce, 2010, *P3M3® – Programme Model,* Version 2.1, p. 2.

delivery of the ICT Reform Program and ICT support to the SRP. The model identifies eight functions that CIOG utilise in its management of ICT services. Figure 4.2 shows the relationships between each of the functions.

Figure 4.2

Overview of CIOG functions

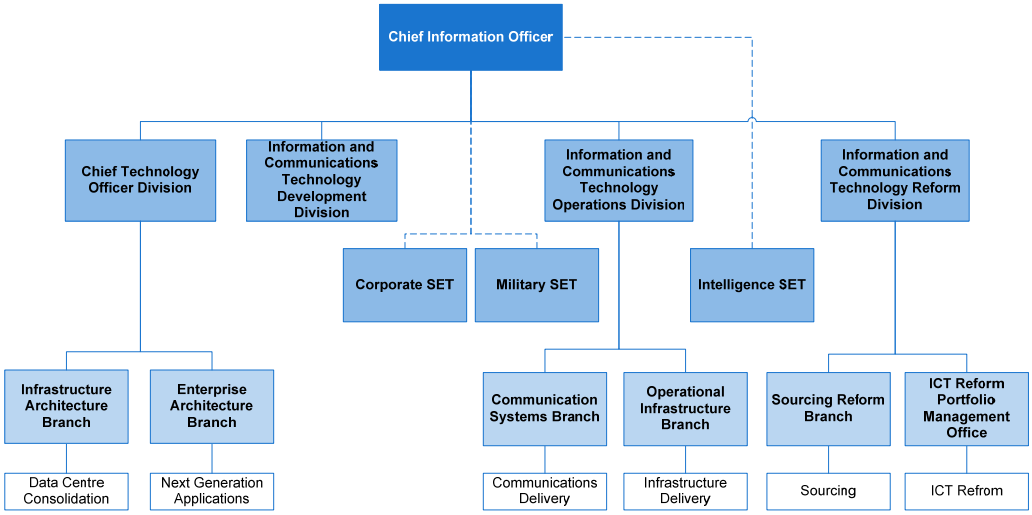


Source: Department of Defence.

4.18 To give effect to its operating model, CIOG is structured as four major divisions reporting to the CIO, each comprising branches responsible for the delivery of ICT projects, as shown in Figure 4.3. Three Stakeholder Engagement Teams (SETs) represent stakeholder priorities and requirements, reporting indirectly to the CIO through the DICTC. To facilitate the implementation of the ICT Reform Program and with the aim of improving accountability, CIOG has divided the IPW across 18 different programs allocated to five Senior Responsible Officers. Each program contains a number of related projects.

Figure 4.3

CIOG management structure



Source: Adapted from Defence documentation.

4.19 CIOG's functions and reporting lines are clear, with projects managed within individual branches, overseen by divisions and by the CIO. The overarching intentions are reasonably clear, projects are clearly assigned to branches, and each branch and division is intended to act as a review checkpoint on the progress of their ICT projects. To improve management control and governance, CIOG has formalised its processes for recording and registering its decisions for further action and future reference.[112] The fundamental requirements for effective management control have been put in place and, as noted by a February 2011 review into the ICT Reform Program (Strategic Assurance Review):

> Considerable progress has been made, in particular in defining the target state and mobilising the CIOG organisation. Stakeholders…noted a significant improvement in [*CIOG*] leadership and staff commitment to ICT Reform.[113]

4.20 However, by that date, it was apparent that CIOG's management processes for trading-off and prioritising competing initiatives were under significant stress. Some 45 per cent of stakeholders, including senior business stakeholders responsible for SRP Streams, cited prioritisation and related

[112] Black, R., *Review of the Defence Accountability Framework*, August 2011, p. 77.

[113] Boston Consulting Group, *ICT Reform – Strategic Assurance Review*, February 2011, pp.4 and 12.

matters as the most significant issues they were encountering in managing ICT investments:

> While senior business stakeholders see the lack of transparency in portfolio decision-making as the single most important issue, this is based upon the view that the greatest risk to delivery is over commitment [*in relation to available capacity*].[114]

4.21 Most stakeholders were of the view that CIOG had insufficient capacity and skills to deliver the full breadth of ICT Reform, that prioritisation processes were not functioning optimally, and that trade-offs were difficult in the absence of the information required for informed decision-making and an agreed set of Defence enterprise-wide priorities. While the causes of these problems may not all lie within the control of CIOG, stakeholders were concerned that CIOG was not actively driving trade-off discussions.

4.22 The findings of the P3M3® assessment of CIOG's management of its portfolio of projects aligned with those of the Strategic Assurance Review, identifying prioritisation as a management process weakness. Although the assessment observed that there was an evolving process for identifying, evaluating and prioritising initiatives, the assessment was that in many cases pieces of processes existed but they were not integrated into a single framework, and were not widely understood.[115]

4.23 Prioritising ICT projects involves considering the value, risk, and the likelihood of realising benefits, and alignment to the intended Defence ICT environment that each project possesses. Accordingly, effective ICT project prioritisation methods are necessary to adequately inform senior management's ICT resource and investment decisions. Defence informed the ANAO in October 2011 that:

> Defence has been conducting trade-off discussions at the two star (Band Two) level but have yet to achieve the level of success required…Defence recognises that the information has not been sufficient to date and CIOG is working to improve this. The establishment of the Applications Managed Service Partnership Arrangement (AMSPA) will help highlight the trade off decisions that are needed.

---

[114] ibid., p. 10.

[115] PCU3ED, *P3M3® Assessment Findings: Department of Defence – Chief Information Officer Group*, Version 1.2, November 2010.

4.24 As noted in paragraph 4.9, the role of CIOG in managing Defence's ICT reform program corresponds to that of a program manager within the overall Defence ICT portfolio. The ANAO's assessment is that CIOG's program-level management control of Defence's ICT investment would be more effective with the benefit of a clearer view of enterprise-wide ICT priorities. Of all Defence Groups, CIOG appears best-placed to inform and coordinate these for consideration at the portfolio level by the Strategic Reform Governance Executive (SRGE) and the Defence Committee. Along with a more activist approach on CIOG's part, this could potentially improve the prioritisation process, aided by a more direct and efficient committee structure and by better definition of CIOG's remit as the coordinating capability manager of Defence's ICT.

Benefits management

4.25 It is important to maintain a consistent focus on the intended benefits and to verify programs and projects remain aligned with the overall strategic direction of the organisation. Benefits management of programs aims to ensure that programs are clearly defined, are measureable, and that the program outcomes are achieved. By critically comparing the risks, costs and benefits for each initiative, program managers can decide which projects require adjustment or should be terminated. It is also important to clearly identify and define benefit dependencies, and to understand how an initiative's outputs will deliver the benefits.

> There should be evidence of suitable classification of benefits and a holistic view of the implications being considered. All benefits should be owned, have realisation plans and be actively managed to ensure they are achieved. There will be a focus on operational transition, coupled with follow-up activities to ensure that benefits are being owned and realised by the organisation. Change management, and the complexities this brings, will also be built into the organisation's approach.
>
> OGC, *P3M3® – Introduction and Guide to P3M3®*, 2010, p. 15.

4.26 The independent P3M3® assessment of CIOG noted that, while benefits management processes were defined for ICT initiatives supporting SRP Streams, the discipline was not consistently applied across all ICT programs. Identification of benefits was inconsistent, robust processes for defining benefits were not in place, and benefits were not being tracked. A significant emerging risk was the slowness in mapping and tracking the interdependencies of ICT projects, notably those critical to the success of one or more SRP Streams.

4.27 Defence first developed high-level maps of SRP interdependencies, including some ICT interdependencies, in September 2010, some 18 months after the SRP got underway. The development of the SRP interdependencies map is consistent with the P3M3® ranking of two for benefits management processes, indicating that there is a localised information structure, with some information sharing between SRP reform streams. The need to track benefits has been recognised, however this process is still in development, as evidenced by the lack of visibility of progress on benefits realisation.

4.28 Subsequent interdependency maps highlight the critical nature of ICT projects and programs in supporting and achieving the intended benefits of the SRP:

- there are a total of 17 interdependent ICT-related projects within the SRP;
- this includes ICT projects supporting four SRP Streams apart from the SRP ICT Stream; and
- of all these, eight ICT-related projects record slippage in the implementation schedule, while nine projects are on-track.

4.29 In addition to the ICT-related initiatives directly aligned with or managed within SRP Streams, as at February 2011, CIOG identified eight SRP Streams with varying levels of dependency on CIOG ICT initiatives to achieve their savings objectives. The dependent SRP Streams are: Non-equipment Procurement, Workforce and Shared Services, Smart Sustainment, Logistics, Preparedness and Personnel Operating Costs, Estate, Army[116] and Reserves. Table 4.2 summarises the number of SRP Streams that are critically dependent on CIOG ICT initiatives.

Table 4.2

Analysis of critical ICT dependencies in the SRP

No. of SRP Streams that are critically dependent on two or more CIOG ICT initiatives	No. of SRP Streams that are critically dependent on one CIOG ICT initiative
7	1

Source: ANAO analysis of Defence data.

[116] Defence informed the ANAO that the main Army ICT dependency is the Defence (Army) Learning Environment, which is managed under the Workforce and Shared Services Stream.

4.30 The critical dependency of eight SRP Streams on CIOG ICT initiatives creates single-point-of-failure[117] risks for more than half of the SRP Streams. The high level of ICT interdependency between SRP Streams introduces the risk that a failure in one SRP Stream will have knock-on effects in other SRP Streams. In these circumstances, where the ultimate delivery of the benefits of the SRP is highly dependent on ICT services and projects to be delivered by CIOG, a high level of accurate and timely information on the progress of ICT initiatives is essential to managing risk. However:

> For the majority of projects, CIOG does not have visibility of when the SRP benefits are to be realised. Hence the desire to synchronise capability development and delivery with benefit realisation is a matter of luck rather than planning.[118]

4.31 This asymmetry in information was confirmed by the February 2011 Strategic Assurance Review, which noted that:

> approximately 40 per cent of the forecast ICT Reform Program benefits are associated with projects or initiatives still lacking bottom-up planning and confirmation. A further 7 per cent of benefits are associated with projects 'requiring remediation', with no evidence that forecast benefits have been adjusted as a result.

4.32 The February 2011 Strategic Assurance Review recommended that CIOG take prompt steps to improve the quality of management information and ensure that interdependencies were understood. This included 'rolling up the sleeves and working collaboratively with project and program teams' to improve or to create the management information necessary to gain a firm view of benefits and of interdependencies. In March 2011, CIOG recommended to the SRP Integration Steering Group that SRP reform streams with CIOG dependencies provide data allowing CIOG to gain visibility of benefit realisation. Defence informed the ANAO in October 2011 that the CIOG Portfolio Management Office was working with a number of projects to identify benefits realisation plans:

> The timing of benefits is not visible yet. This is because individual reform streams are responsible for timing and development of reform activities within

[117] A single-point-of-failure is a part of a system, project or program that, if it fails, will stop the entire apparatus from working. They are undesirable in any system that aims for high availability, whether a network, a software application or other industrial system.

[118] SRP Integration Steering Group, March 2011 – *ICT Support to SRP Streams*.

> their own streams and with it, the specific user requirements. Only when the specific user requirements have been developed will the timing of ICT benefits become visible.
>
> The nature of specific interdependencies will become clearer as the [*SRP*] Streams are able to articulate in more detail, with CIOG's help, their actual ICT requirements.

4.33 The ANAO's assessment is that the P3M3® maturity ranking of two allocated by the independent assessor for CIOG's benefits management capability, while understandable, tends to underplay both the critical importance of the process in the context of the SRP and the barriers to improving performance. The lack of CIOG oversight of all ICT benefits realisation plans reflects, in part, the incomplete integration of CIOG into the SRP portfolio governance process. While ICT is an essential enabler of major SRP Streams, CIOG has not always been incorporated as a full partner into those SRP Streams with heavy dependencies on ICT initiatives. The need for a comprehensive benefits realisation framework is manifest and a requirement for the timely and effective management of the SRP and ICT reform.

Financial management

4.34 In the P3M3® framework, financial management focuses on ensuring that sufficient funding is available and that program costs are adequately detailed, categorised and managed throughout the program's life cycle.

> There should be evidence of the appropriate involvement of the organisation's financial functions, with approvals being embedded in the broader organisational hierarchy. The business case, or equivalent, should define the value of the initiative to the business and contain financial appraisal of the possible options. The business case will be at the core of decision-making during the initiative's life cycle, and may be linked to formal review stages and evaluation of the cost and benefits associated with alternative actions. Financial management will schedule the availability of funds to support the investment decisions.
>
> OGC, *P3M3® – Introduction and Guide to P3M3®*, 2010, p. 15.

4.35 The CIOG Internal Operating Model identifies a financial management sub-function responsible for the strategic allocation and tracking of financial resources in CIOG.[119] The role of the financial management sub-function is to track work-effort and confirm proper expenditure of CIOG funding through information from the Program Information Templates and from Defence's financial management tools (such as the primary budgeting and financial reporting tool—BORIS—and the personnel management tool—PMKeys).

4.36 Under the P3M3® framework, the independent assessor ranked CIOG's financial management maturity as two, identifying the existence of a defined process for approving ICT initiatives, and noting progress that CIOG had made in establishing processes for identifying and approving ICT initiatives. However, the independent assessor also commented that:

> The approval process used varies according to the funding source, with no 'CIOG' process which pulls together internal, wider Defence and Whole of [*Government*] processes into a single integrated framework.[120]

4.37 This was borne out by the ANAO's examination of a sample of ICT projects submitted for approval to DICTC. The ANAO's examination focused on the completeness and quality of information in the project business cases presented to the DICTC for consideration, and the outcomes were mixed. Of the 16 ICT proposals examined, nine were submitted in the approved business case format, containing all the required information for consideration by decision-makers. The quality of the financial information varied widely, with some business cases presenting detailed cost estimations over the life of the project along with the anticipated benefits, while others only provided a brief mention of anticipated overall project costs. As discussed in Chapter 2,

---

[119] Defence informed the ANAO in October 2011 that:

> 'The CIO Group maintains a Group Finance Office (GFO), which was established in 2004 with the formation of the CIO Group. The GFO is arranged with the following framework: A centrally pooled level of financial analysis, around IPW program and IPW project budget allocation and performance reporting.
>
> This is supplemented by embedded finance project staff in IPW projects or programs performing detailed estimates, scheduling, financial risk monitoring and reporting at project task level together with procurement order activities on ROMAN (all reporting to GFO); and a centrally pooled and assigned finance costing team (not reporting to GFO) who are responsible for detailed cost estimates over the life of the project but as an assurance function only.'

[120] PCU3ED, *P3M3® Assessment Findings: Department of Defence – Chief Information Officer Group*, Version 1.2, November 2010, p. 16. As noted in paragraph 2.66, Defence is in the process of finalising a Defence ICT investment two-pass approval process in consultation with the Department of Finance and Deregulation.

Defence informed the ANAO in October 2011 that it was in the process of finalising a Defence ICT investment two-pass approval process in consultation with Finance and that the variations the financial information provided in the business cases:

> reflects that financial decision-making at the departmental level is at the WFMC, and not the DICTC, and so there is a lesser requirement for financial analysis to be presented to the DICTC.

4.38 The independent P3M3® assessor noted that the consequent cost tracking and forecasting was inconsistent across projects and that CIOG was still developing effective forward planning for funding availability. By February 2011, the Strategic Assurance Review confirmed that senior stakeholders, including SRP stakeholders, were concerned by capital planning that was apparently limited to the current financial year. Planning for forward funding had become critical, to the extent that ICT projects had collectively underspent their allocated budgets. At that time, at least $95 million (or approximately 50 per cent) of annual project funding had yet to be committed before the end of 2010–11. Defence informed the ANAO in December 2011 that:

> As ClOG has matured, a number of different costing models and methods have been used in ClOG, with inconsistent results. ClOG faces increasing pressure to apply a single, consistent and robust ICT costing methodology to projects that will be approved via the DCP, the new Defence ICT Investment Approval Process (DIIAP), or Minor Capital project processes.

4.39 The Strategic Assurance Review confirmed that the underspending of project budgets was primarily due to persistent delays in the rollout of ICT reform projects, placing at risk the realisation of benefits:

> Many known project delays are not fully reflected in the forward investment plan, potentially pushing investment into [*2012–13*] (where CIOG is already over-committed) or beyond…As available investment dollars drop off dramatically after [*2012–13*] CIOG's ability to re-allocate funding between projects may be restricted as the investment budgets decrease from 2012–13 onwards, especially if other SRP Streams also experience delays.

4.40 In the event, CIOG overspent its budget in 2010-11. As discussed in Chapter 3 (at paragraph 3.28), it did so by:

> investing in the replacement of end-of-life Data Centre infrastructure, accelerating other projects in the IPW to satisfy customer demands and bringing forward annual software licensing renewals to take advantage of

early payment discounts and relieve financial pressure in the next financial year.[121]

4.41 CIOG's financial management processes recently achieved a portfolio-level P3M3® maturity ranking of two. Considered at the program level within the portfolio of Defence business, this corresponds to processes under which:

> …business cases are produced in various forms and the better and more formal cases will present the rationale on which to obtain organizational commitment to the programme. Overall cost of the programme is not monitored or fully accounted for.[122]

4.42 Having recently achieved this degree of maturity, there remain substantial challenges to CIOG consolidating and improving the effective financial management of ICT initiatives. As many ICT initiatives are essential and critical enablers of SRP streams, there is strong incentive to elevate financial management processes so as to ensure that CIOG is capable of supporting Defence's portfolio of ICT investment. This would entail CIOG putting in place centrally established standards for the preparation of ICT business cases, along with processes for their management throughout the program life cycle and across programs. In October 2011, Defence informed the ANAO that:

- a centrally established business case template is being developed by the dedicated whole-of-government team;
- a dedicated ICT costing team is developing a standard ICT costing methodology;
- the Project Management Centre of Excellence has been established to formalise standard project management doctrine for CIOG projects; and
- the PMO continues to provide whole-of-life monitoring across all of the 18 ICT programs.

4.43 While CIOG has an important role to play, it is also worth considering the maturity of Defence's portfolio-level financial management processes for these programs. At this time, they are likely to align with those of CIOG, in that business cases are being produced and some, usually departmental,

---

[121] Defence, *Strategic Reform Program Performance Report for the Period January to June 2011*, August 2011, p.12.

[122] UK Office of Government Commerce, 2010, *P3M3® – Programme Model,* Version 2.1, p. 8.

structures are in place to oversee investment decisions. This assessment of Defence's portfolio-level financial management processes corresponds to a portfolio-level P3M3® maturity of two, at which:

> …business cases are often appraised independently of each other and real organizational priorities have not been established.[123]

4.44 At this point in time, there would be benefits from the exercise of a portfolio-level responsibility, somewhat beyond CIOG's remit, to ensure that ICT planning processes are integrated and consistent with a Defence portfolio view of its major programs, including the portfolio of SRP programs represented by the SRP Streams.

Stakeholder engagement

4.45 The engagement of stakeholders, both within and external to the organisation, is critical to the success of a program. Best practice is for stakeholders to be effectively engaged in order to obtain their support and feedback.

Stakeholder engagement includes communications planning, the effective identification and use of different communications channels, and techniques to enable objectives to be achieved. Stakeholder engagement should be seen as an ongoing process across all initiatives and one that is inherently linked to the initiative's life cycle and governance controls.

OGC, *P3M3® – Introduction and Guide to P3M3®*, 2010,p. 15.

4.46 CIOG has developed a Communication, Marketing and Change Strategy (Communications Strategy) to inform CIOG staff, the broader Defence community and external stakeholders of how organisational change resulting from the ICT Reform Program is intended to be managed. The Communications Strategy outlines the communication channels in which information on the ICT Reform Program will be broadcast to stakeholders, including:

- through SETs;
- by conducting internal workshops;
- by presenting briefings to industry;

[123] UK Office of Government Commerce, 2010, *P3M3® – Portfolio Model*, Version 2.1, p. 8.

- via an ICT reform intranet site; and
- through articles published in Defence magazines.

4.47 Many of these communication initiatives have been implemented. The CIOG executives regularly conduct briefings with industry, providing information on the goals of the ICT Reform Program along with updates on specific projects being undertaken. A CIOG intranet site has been developed which provides Defence staff with updates on key ICT reform activities.

4.48 The Communications Strategy outlines the establishment of a directorate within the ICT Reform Branch of CIOG, called the Directorate of Communications and Change Management Reform (DCCMR). The DCCMR is responsible for implementing and marketing the organisational changes arising from the ICT reform program and designing and targeting communication methods to promulgate them, such as cultural change workshops. Defence informed the ANAO in October 2011 that since March 2011, over 500 staff have attended these workshops.

4.49 On the basis of these processes for stakeholder engagement, the independent assessor assigned a ranking of two to the maturity of CIOG's stakeholder management processes. The independent assessor also noted that:

- beyond initial engagement by SETs, the wider processes for stakeholder management were not well-defined or consistently applied;
- once a project is approved, communications were typically devolved to the project level and became fragmented; and
- there were limited alternatives to communicating issues aside from the formal processes.[124]

4.50 The February 2011 Strategic Assurance Review confirmed that senior business and CIOG stakeholders (including SRP stream business managers) reported an improvement in CIOG's understanding of business needs over the previous 12 months. In particular, CIOG had:

> Improved its responsiveness to the business by continuing to build on the progress made by SETs and the Enterprise Solutions Branch (ESB), both established in 2009.[125]

---

[124] PCU3ED, *P3M3® Assessment Findings: Department of Defence – Chief Information Officer Group,* Version 1.2, November 2010, p. 17.

[125] Boston Consulting Group, *ICT Reform – Strategic Assurance Review*, February 2011, p. 5.

4.51 However, business stakeholders were seeking more transparency and engagement from CIOG in respect of project scheduling, progress and delivery. The focus of stakeholder concerns was the CIOG's role in discussing and facilitating the process of setting priorities for ICT investments; and stakeholders were looking for more strategic discussions at the DIEC and DICTC. They considered that current discussions were too focused on details to be considered effective and business stakeholders lacked the lead times and information needed to give advice to support informed decision-making.

4.52 The maturity ranking of two assigned to CIOG's process for managing stakeholder engagement corresponds to the general criterion set out by OGC for this maturity level:

> Some programmes will be communicated to stakeholders, but this is linked more to the personal initiative of programme managers than to a structured approach being deployed by the organization.[126]

4.53 The ANAO considers that CIOG has put in place the fundamental elements of stakeholder engagement and communications needed to support a broad ICT Reform Program and the SRP. Having achieved a basic level of communications capability, the challenge facing CIOG is to improve its communication with its main business stakeholders (especially in respect of project delivery and timing) to provide more visibility on project progress and priorities, as well as elevating its support to DIEC and DICTC to a more strategic level.

Risk management

4.54 At the program level in the P3M3® management maturity framework, the main focus is on the arrangements to ensure that a balance is achieved between the threats to, and opportunities presented by, the program; thereby giving stakeholders confidence that program objectives will be fulfilled.

> Responses to risk will be innovative and proactive, using a number of options to minimise threats and maximise opportunities. The review of risk will be embedded within the initiative's life cycle and have a supporting process and structures to ensure that the appropriate levels of rigour are being applied, with evidence of interventions and changes made to manage risks.
>
> OGC, *P3M3® – Introduction and Guide to P3M3®*, 2010, p. 15.

[126] UK Office of Government Commerce, 2010, *P3M3® – Portfolio Model,* Version 2.1, p. 11.

4.55 The PDM incorporated responsibility for program-level risk management with DICTC and the Strategic Reform Governance Executive (SRGE). Under the arrangements set out in the PDM, each project has an Issues and Risk Register, maintained by CIOG's Directorate of Group Governance and Reporting (the Directorate-see paragraph 3.32). One of the responsibilities of the Directorate is to identify, collect, classify, assess and track project-level issues and risks and elevate them to the DICTC and SRGE at the program-level.

4.56 CIOG's independent P3M3 assessor noted the existence of the risk register, the ICT Reform Office's role in analysing risks and mitigation plans, the escalation of risks to the Defence Audit and Risk Committee when required, and the practice of reporting project risk to the SRGE and DICTC through Project Status Reports. These features meet the requirements for a maturity ranking of two for risk management processes.

4.57 The weaknesses in risk management processes noted by the assessor extended to the lack of a systemic process for analysing and escalating project and program risk (including to the portfolio level), and the patchy quality of risk management processes within ICT projects. The strengths and weaknesses of CIOG's risk management processes were also observed by the February 2011 Strategic Assurance Review. For instance, CIOG's own assessment at the time had identified:

> 40 per cent of projects…[*are*] 'at risk' or 'requiring remediation', while the remainder [*were*] 'green' or largely on track. [*CIOG*] has developed an independent view on the status of the 'top 15 projects', with 14 of these projects regarded as 'at risk'.[127]

4.58 Notwithstanding the development of risk identification, monitoring and reporting processes, the Strategic Assurance Review found:

> [*CIOG's*] effectiveness in managing portfolio-wide issues and risks is hindered by inadequate escalation procedures, with many critical concerns escalated to key decision-makers late in the process or not at all.[128]

4.59 CIOG's processes for managing risk are consistent with those of a program management organisation that has just achieved a maturity level at which risk management is recognised and used but there are inconsistent

[127] Boston Consulting Group, *ICT Reform – Strategic Assurance Review*, February 2011, p. 8.

[128] ibid., p. 16.

approaches, and varying levels of commitment and effectiveness. The need for attention and improvement appears to be recognised by CIOG, which has achieved some initial successes that warrant active pursuit and improvement. The pressing issue identified by both the P3M3® assessor and the Strategic Assurance Review is the need for a portfolio-wide consistent approach to escalating and treating ICT program and project risks. Defence informed the ANAO in December 2011 that:

> Project Management Centre of Competence has commenced work in standardising templates, tools, etc. Also identifying when program/project risks should be escalated to Group level.

Organisational governance

4.60 Organisational governance is the framework established by a governing body to provide stakeholders with the assurance that the organisation is performing its responsibilities with due diligence and accountability. In the context of P3M3®, the role of organisational governance is to align the delivery of initiatives to the organisation's strategic direction. It is concerned with controlling and mitigating the impact of external factors, and is distinct from management control, which focuses on how internal control is maintained.

> [*Organisational Governance*] looks at how the delivery of initiatives is aligned to the strategic direction of the organisation. It considers how start-up and closure controls are applied to initiatives and how alignment is maintained during an initiative's life cycle.
>
> Organisational governance also looks at how a range of other organisational controls are deployed and standards achieved, including legislative and regulatory frameworks. It also considers the levels of analysis stakeholder engagement and how their requirements are factored into the design and delivery of outputs and outcomes.
>
> OGC, *P3M3® – Introduction and Guide to P3M3®*, 2010, p. 16.

4.61 In its efforts to improve ICT capability management, Defence has taken steps to align its governance structures with good practice. As previously mentioned in Chapter 2, the Secretary and the CDF established the DICTC to provide strategic-level input for the redevelopment of Defence ICT capacity. The DICTC is at the apex of a structure of committees focussing on more specific aspects of developing ICT capacity and managing ICT investments.

4.62 As previously mentioned in paragraph 2.20, a PMO has been established by CIOG to prioritise future ICT investment proposals, report on project status, allocate resources and provide financial benefit forecasts. CIOG

has also developed a Defence ICT Target Operating Model, which outlines, at a high level, the interactions between the parties involved and the ways in which they work together in delivering ICT shared services to Defence.

4.63 CIOG's P3M3® assessor noted the establishment of an executive board structure to oversee and review project performance; that the ICT reform program was aligned with Defence's strategic objectives and priorities; and that processes for identifying, evaluating and prioritising initiatives were developing. The stakeholders interviewed as part of the February 2011 Strategic Assurance Review reported that the CIOG Senior Leadership Team appeared to be effective and strongly committed to ICT reform, with leadership behaviour being increasingly demonstrated.

4.64 However, as discussed in Chapter 2, DICTC is not well-integrated into the decision-making structure of the major portfolio of work being undertaken under the SRP. Neither is it properly integrated into Defence's accountability structures, the apex of which is the Defence Committee jointly chaired by the Secretary of Defence and CDF. The August 2011 *Review of the Defence Accountability Framework* (the Rufus Black Review) observed that:

> subordinate committees to the Defence Committee [*including the*] Defence Information, Capability and Technology Committee (DICTC) … do not formally report to the Defence Committee. There appears to be no mechanism by which decisions in the Defence Committee bind decisions in these subordinate committees or vice versa.[129]

4.65 CIOG's P3M3® assessor found that, while CIOG's higher level governance structures were in place, its organisational governance structures had not been bedded down. The subsequent February 2011 Strategic Assurance Review found that DICTC had limited visibility of important program-wide metrics, including ICT costs and resources. Consequently, DICTC exercised little influence over the prioritisation of ICT projects and was effectively functioning as a consultative group rather than strategically driving the delivery of the ICT Reform Program.

4.66 This review also identified that organisational governance structures had not developed significantly below the executive level, so that inconsistent approaches were being taken by different programs and projects. A common, documented approach with established policies, standards and process had yet

[129] Black, R., *Review of the Defence Accountability Framework*, August 2011, p. 37.

to be established and promulgated. An indicator of the functional level of maturity achieved was the review's assessment that the PMO had yet to achieve the effective management of portfolio-wide issues or provide the best available information to decision-makers due, in part, to inadequate escalation procedures:

> given the size and complexity of the ICT Reform Program, we would expect a strongly functioning, 'activist' PMO to be in place at this stage.[130]
>
> Some ambiguity remains on the role of the ICT Reform PMO, despite recent confirmation of the role by the CIOG Executive. Delays in the PMO's establishment are in large part responsible for the lack of clarity around the roles and accountabilities of key portfolio planning and work take-on functions such as the SETs, ESB and the planning functions in ICTDD [*Information Communications Technology Development Division*] and ICTOD [*Information Communications Technology Operations Division*]. As a result, divisional silos have persisted as a necessity and the cross-CIOG collaboration needed for the ICT Reform Program has not been established.[131]

4.67 Defence informed the ANAO in December 2011 that:

> Over the past six months, to improve CIOG's integrated view of its program of work, it has developed a Master Schedule which depicts the progress of key projects within CIOG's IPW. The Master Schedule focuses on the top 20 IPW projects with cash bearing benefits. The data contained in the Master Schedule includes key project milestones such as key approval dates, product delivery points, Exception Report approvals, benefits realisation points, project status rating and resource supply status rating.
>
> The information provided by the Master Schedule is being used by the Portfolio Management Office as: a lead indicator in preparing for future project needs and developments; a decision support and management tool to independently make recommendations to programme SROs [*Senior Responsible Officers*] and the CIOG Executive; [*and*] a driver for the escalation of projects requiring remediation, as part of the mandated CIOG Exception Reporting process.

4.68 The February 2011 Strategic Assurance Review found that in practice, effective governance was complicated by the variability in the performance information reported for major ICT projects. The review assessed the

[130] Boston Consulting Group, *ICT Reform – Strategic Assurance Review*, February 2011, p. 15.

[131] ibid., p. 12.

implementation of the Defence ICT Target Operating Model and its supporting processes as incomplete in a number of areas, resulting in ongoing 'friction points' within CIOG:

> The new way of working has not fully cascaded down CIOG. Many CIOG stakeholders believe that senior leaders understand the target model but those further down the organisation do not understand its impact on individuals' roles and what they need to do differently—in other words, the direction has not yet been translated into day-to-day activities at an operational level.[132]
>
> CIOG support processes are inconsistent and seen as barriers to getting work done. While the root cause is unclear and likely involves responsibilities in both the central functions and the Divisions, funding allocations, procurement approvals, recruitment processes, resource allocation and accommodation provisioning are all raised by CIOG stakeholders and project managers as impediments to project initiation and delivery.[133]

4.69 Accordingly, the February 2011 Strategic Assurance Review recommended that Defence increase focus and sharpen the accountability for the approval processes by documenting the requirements for the various approval processes in a decision tree. CIOG reported to the Defence Audit and Risk Committee in May 2011 that the approval process had been drafted in a decision tree format but was not yet published. Defence informed the ANAO in October 2011 that work on the approval process was still continuing and is yet to be finalised. Defence further informed the ANAO in December 2011 that:

> CIOG is supporting the Strategic Reform Program, which includes undertaking major process reform within the Group. Changes of this scale are disruptive by nature. CIOG has an extensive internal communications program to ensure that all staff understand the change journey.

4.70 The organisational governance supported by CIOG remains, in the ANAO's view, in its early stages of development. The P3M3® ranking of two awarded by the independent assessor reflects a state in which organisational controls are only just starting to take shape but remain largely *ad hoc* and without the benefit of strategic control. For organisations involved in lower risk activities, this state might be tolerated for some time. However, CIOG is directly involved in or is a de facto partner in five of the significant SRP streams charged with delivering fundamental organisational reform and

[132] ibid.

[133] ibid., p. 13.

substantial savings, in addition to significant programs of ongoing work to support operations, procurement and sustainment. In these circumstances, there is a real need for CIOG to strengthen its organisational governance arrangements, to support the effective functioning of high-level governance bodies (including DICTC and the SRGE), and to clarify accountability.

Resource management

4.71 Resource management involves the efficient and effective management of all types of resources—including equipment; inventory; information; and human resources—in the delivery of organisational programs. A primary factor in resource management is the process for acquiring resources and how supply chains are utilised to maximise their effective use.

> There will be evidence of capacity planning and prioritisation to enable effective resource management. This will also include performance management and exploitation of opportunities for greater utilisation. Resource capacity considerations will be extended to the capacity of the operational groups to resource the implications of change.
>
> OGC, *P3M3® – Introduction and Guide to P3M3®*, 2010, p. 16.

4.72 The delivery of ICT Reform Program initiatives has been subject to human resource constraints. In December 2009, the PDM highlighted the strain that the reform activities would place on CIOG:

> [*The*] aggregate demand for CIOG project resources is forecast to be double current supply until [*the second quarter of 2011–12*].[134]

4.73 The likely demand for human resources was anticipated to outstrip the available supply so that, by the first quarter of 2010–11, there would be an anticipated shortfall of 400 full-time employees. To avert the shortfall, CIOG commissioned further analysis and received a plan from the consultant that indicated the potential to reduce the anticipated shortfall to 10 full-time staff, as shown in Table 4.3.

[134] Department of Defence, Chief Information Officer Group *Defence ICT Reform Program Design Manual*, December 2009.

Table 4.3

2009 proposed plan to address the resource shortfall

Planned action	Full-Time Equivalent staff reduction
Delay selected projects	20
Rigour test project requirements	130
Reallocate resources from business-as-usual to reform	100
Assign existing project resources to 'best fit' roles	50
Increase outsourcing	70
Fill vacancies in Reform Team, cancel other vacancies	20

Source: Department of Defence.

4.74 Subsequently, a flexible resource model was developed by CIOG in 2010, as a response to the recognition of CIOG's lack of capacity to strategically focus its resources to the extent needed to support and enable ICT reform activities. The resource model was based on the principle of matrix management, so that all CIOG employees working on ICT projects would be available for placement in priority projects across the Group as and when required.

4.75 The steps taken by CIOG reflect the development of methods to identify and track resource supply and demand, improvements in the quality of data and the staffing estimates supplied to CIOG by projects, and better central oversight of skills and competencies. CIOG comfortably achieves the requirements for a resource management maturity ranking of two, consistent with these developments. Improving the maturity ranking would involve:

- monitoring and guiding resource allocation at the whole-of-CIOG level;
- better matching resources to demands and skills to positions through more effective staffing and contracting processes; and
- improving staff training and the induction of project managers.[135]

[135] PCU3ED, *P3M3® Assessment Findings: Department of Defence – Chief Information Officer Group,* Version 1.2, November 2010, p. 19.

4.76 As of March 2010, CIOG's estimated resource shortfall stood at 350 full-time equivalent staff, and CIOG undertook further work to ensure that projects were appropriately prioritised. However, the impact of resourcing constraints and sub-optimal practices for managing supply and demand continued to be evident in the February 2011 Strategic Assurance Review, which found that:

> Reallocation of the current workforce appeared impractical (in particular, shifting sustainment resources to projects), given the shortage of the skills required to drive major projects and the lack of transparency around staff capabilities and rostering;
>
> Dramatically changing the skill mix appears unlikely in the short term as overall [*Australian Public Service fulltime employees*] limitations constrain the amount of change possible in any given period and recruitment processes often involve significant lead times; and
>
> CIOG lacks the capability to increase its reliance on the market to deliver key projects (or sustainment activities) in the short term, due to delays in establishing new sourcing arrangements (caused in large part by failure to properly resource the projects to establish these) and a lack of commercial and vendor management resources to support high levels of sourcing activity.[136]

4.77 Further, the review reported that senior CIOG stakeholders saw the over-commitment of resources, in particular resource capacity and allocation issues as the most significant challenge facing the delivery of the ICT Reform Program. At the time, an analysis of 25 projects found that 44 per cent were under-resourced, notably in respect of technical resources (58 per cent) and project managers (40 per cent).[137] Resource constraints were also identified as a key factor in causing delays in start-up of ICT projects, raising risks to achieving project outcomes:

> Where the PMO has recent self-assessment reports, 40 per cent of projects report their status as 'at risk' or 'requiring remediation' … The PMO has developed an independent view of the status of the 'top 15 projects', with 14 of these projects regarded as 'at risk'.[138]

4.78 The short to medium-term options open to CIOG include removing its internal silos inhibiting staff movements between its divisions, lifting its

[136] op. cit., Boston Consulting Group, p. 12.

[137] ibid., p. 8.

[138] op. cit., Boston Consulting Group, p. 8.

resource capacity by temporarily drawing on industry capability, fast-tracking the APS recruitment of people with skills in demand, and centrally pooling experienced project and program managers, business analysts and other personnel with 'hot skills'. In an effort to address the workforce shortfall, CIOG informed the ANAO in October 2011 that:

> …to date, CIOG has released over 100 full time employees from sustainment activity to project activity without materially impacting on the delivery of services. CIOG is also seeking additional resources from within Defence and has established the AMSPA [*Applications Managed Service Partnership Arrangement*] to further increase CIOG's capacity.

4.79 However, more enduring solutions to ICT resourcing problems will require a broader view of the resources available and the personnel required to meet all of Defence's wider ICT priorities. The steps that can be taken in the short and medium-terms are useful to support the development of a more considered resource management plan, though they are unlikely to be sustainable in the longer term.

4.80 A more considered approach would involve CIOG fully scoping the scale and complexity of many of the proposed ICT reform activities, including the major programs of work being undertaken by the SRP Streams. The most recent available data shows little recovery of the current schedule slippage of ICT initiatives supporting the SRP Streams, and continuing increases in slippage in the project schedules for the IPW. In the present state, the majority of timeframes suggested for implementing ICT reforms remain as originally estimated and have yet to adjust to the feedback from program and project managers, showing delays in start-up and ongoing resource shortfalls.

4.81 While slippage typically results from a number of contributing causes, the underlying factor in implementing ICT reform initiatives to date has been the underestimation of the demand that was placed on finite ICT resources within CIOG and other Defence groups. The 2018–19 deadline for achieving the outcomes of the SRP has tended to drive CIOG's resource management on a case-by-case basis, rather than fostering management at a strategic level.

4.82 Defence informed the ANAO in December 2011 that:

> Resource management has been prioritised as an area that requires immediate improvements and over the past 12 months CIOG has introduced a flexible resource model, and aligned all investment resources to dedicated Streams (e.g. project managers, business analysts) to improve transparency and control over the resource supply and demand picture.

The need for improved portfolio and program management maturity

4.83 CIOG's management structures and processes have developed significantly since its inception in 2004, particularly since being designated as the coordinating capability manager for Defence's ICT. From the state of affairs at the time of the 2007 Defence Management Review (DMR),[139] when a CIO had yet to be appointed,[140] CIOG has developed an ICT strategy document which was released in November 2009, proposed a Defence ICT Architecture in 2010 and taken steps to manage the transition to a Defence-wide information environment. These are important achievements for a Defence organisation that is moving towards remediating substantial defects and deficiencies in its information systems and their management.

4.84 Within the P3M3® framework, CIOG's current management maturity assessment of two is in accord with the steps that have been taken to lift Defence's management of ICT from a very low base up to a level comparable with many other organisations. The ANAO's examination of CIOG's performance suggests that, having attained this level of performance, priority needs to be given to further improving management processes if CIOG is to consolidate its achievements and manage the significant emerging risks:

- CIOG has a key role to play in setting priorities for ICT programs and projects in conjunction with senior business stakeholders. A more activist CIOG would be better placed to provide the information and support that senior decision-makers require if they are to set priorities for Defence as a single entity.
- Improving the quality of management information and fully understanding interdependencies is a key task facing CIOG if it is to effectively support the setting of priorities and the monitoring of the intended benefits of ICT programs and projects. This means 'rolling up the sleeves and working collaboratively with project and program teams' to improve or create the management information necessary to gain a firm view of benefits and of interdependencies.

[139] Also known as the Proust Review.

[140] The CIO was appointed in 2007.

- Promulgating and adopting consistent business case requirements, along with improved financial management and financial monitoring tools, will assist CIOG and decision-makers manage Defence's wider portfolio of ICT initiatives, and set a firm base for weighing the costs and benefits of ICT proposals at the program and portfolio levels.
- Having put in place the essential elements of a communication strategy, the challenge facing CIOG is to consolidate the progress to date, improve communication with its main business stakeholders, and to provide more visibility on project progress and priorities to senior decision-makers.
- There is a pressing need for a more consistent approach to monitoring and managing ICT risks. The basic processes are largely in place, though the processes and pathways for the timely escalation of risks to senior decision-makers are not well defined and give rise to inconsistent outcomes.
- There is a real need to re-assess the resources required to deliver the full program of ICT reform currently set out by CIOG, including in support of the SRP. Resource pressures are acute, and personnel shortfalls are evident. Program and project timelines have yet to be realistically adjusted in light of the available resources, and a viable plan for the longer-term management of resource requirements is yet to be developed.
- CIOG's organisational management processes are not sufficiently developed to effectively support its heavy involvement in supporting SRP Streams, operations, procurement and sustainment. The risks involved to Defence as an enterprise are significant and a rapid increase in the maturity of organisational management in accountability structures appears necessary.

4.85 The ANAO acknowledges that external independent reviews have submitted recommendations to Defence regarding some of the above mentioned risks, which Defence is in the process of addressing.

Recommendation No.1

4.86 The ANAO recommends that, to address emerging risks in the delivery of ICT support to Defence business, Defence:

(a) clarify the role of CIOG as an ICT service provider and coordinating capability manager of Defence ICT; and

(b) ensure that Defence program managers and SRP streams adopt a full partnership model with CIOG to deliver relevant Defence portfolio initiatives.

Defence response: Agreed.

Portfolio-level implications

4.87 The implications and ramifications of improving CIOG's current level of management maturity are far-reaching and highlight the need for a higher-level portfolio view of Defence's portfolio of management activities. From the perspective of the management of ICT, effective portfolio-level management is necessary to manage key risks, including resource risks, financial risks, and the risks to enterprise-wide goals that might result from a single ICT failure.

4.88 As noted in Table 4.2, seven major SRP Streams depend for their success on two or more common ICT projects, or on conjunct elements of those projects. The failure or even the significant delay of one of these projects could have a domino effect on other SRP activities that may delay or deny the anticipated flow of SRP savings into improved Defence capability.

4.89 Such concerns are evident in the comments of senior business stakeholders in the course of the February 2011 Strategic Assurance Review. They cited a lack of appropriate portfolio, program and project management information, including leading indicators on progress, a portfolio-wide view of interdependencies, and benefit realisation tracking against an agreed framework.[141]

[141] Boston Consulting Group, *ICT Reform – Strategic Assurance Review*, February 2011, p. 15.

4.90 The need for active portfolio-level management is also evident in the current confused accountability structures interposing the DICTC between the CIO and the SRGE, without a clear line of enterprise-level accountability to the Defence Committee. As noted in the recent Black Review, the need for a more direct, effective and efficient committee structure is not confined to Defence's management of its ICT:

> There are too many committees in Defence, which create diffused and confused accountability and their operation is often characterised by poor procedures.[142]
>
> …the current arrangements constrain leadership capability and management capacity by reducing the ability of decision makers to exercise strategic control over the construction and implementation of decisions. This can manifest in loss of visibility of implementation, dispersion of implementation with insufficient monitoring or tracking, separation of decision authority from responsibility for implementation, or decision-making authority residing with more than one entity, any of which may act without reference to broader interests or policies.[143]

[142] Black, R., *Review of the Defence Accountability Framework*, August 2011, p. 9.

[143] ibid., p. 14.

Recommendation No.2

4.91 The ANAO recommends that, to improve the portfolio-level view of Defence's enterprise needs and to support the achievement of the challenging goal of managing Defence as a single entity, Defence:

(a) establish an enterprise-wide benefits realisation framework;

(b) ensure it has in place appropriate financial systems to support the effective planning and monitoring of ICT investments; and

(c) develop a consistent, portfolio-wide approach to escalating and treating ICT program and project risks.

Defence response: Agreed.

Ian McPhee
Auditor-General

Canberra ACT
20 December 2011

Appendices

Appendix 1: Reviews of Defence ICT

***2007 Defence Management Review* (DMR):** The DMR examined and assessed organisational efficiency and effectiveness in Defence. It made 10 recommendations on Defence's management of the Defence Information Environment. The two key recommendations were that Defence appoint an expert CIO, and develop an ICT strategy and business plan.

***2008 Audit of the Defence Budget* (DBA):** The DBA analysed Defence's finances, operations and management processes, as well as its major cost drivers, in order to find opportunities for efficiencies and reinvestment. The overall conclusion of the audit was that deep reform was required in Defence, and it made 16 recommendations in relation to ICT that were consistent with those made in the DMR.

***CIO review of ICT*, 2008:** The newly appointed Defence CIO commissioned Booz & Company to assess the current state of the Defence ICT environment. The resulting report *Defence ICT Strategy – Phase I Executive Summary* found 18 key weaknesses across the ICT operating model, including weaknesses in portfolio management processes, governance and data resulting in inefficient prioritisation of initiatives; low initiatives management maturity resulting in inadequate initiatives management and sub-optimal delivery of outcomes; and poor ICT workforce planning processes had resulted as a consequence of limited visibility of ICT resources, funds, processes and outcomes. The report outlined four strategic imperatives aimed at improving Defence's ICT capabilities that Defence could adopt, which subsequently formed the basis of the DICT Strategy.

***Defence White Paper – Information and Communications Technology Companion Review*, 2008:** The ICT Companion Review aimed to summarise Defence's ICT issues out to 2030, in addition to providing input into the 2009 Defence White Paper. The review found that the Defence ICT environment was unacceptably fragile, fractured and ungoverned and required fundamental change to the governance, planning and control frameworks as well as investment in critically under-funded capabilities.

***Review of The Australian Government's Use of Information and Communication Technology* (Gershon Review), 2008:** At a whole-of-government level, the Department of Finance and Deregulation commissioned Sir Peter Gershon to undertake a review on the efficiency and effectiveness of the Australian Government's use of ICT. The report outlined a plan for

improvements to governance, capability, ICT spending, ICT skills, data centres, efficiency and effectiveness, and sustainability of ICT. Although Defence was not officially a subject of the Gershon review, the DICT Strategy states that 'the Secretary of Defence maintained contact with Sir Peter Gershon throughout the strategy development process and that its ICT reform initiatives are 'consistent with the recommendations in the Gershon Review … and the outcomes sought from that review'.

Appendix 2: Major ICT Initiatives

Table A 1

Major ICT Initiatives

Strategic Imperative	Initiative	Description	Planned implementation date	Current status
Optimise Defence ICT investment	Data Centre Consolidation	The Defence Information Environment supports 200 data centre/server rooms at significant cost. The aim of this initiative is to increase efficiencies and reduce cost by consolidating the data centres to less than 10.	2016–17	Five year lease of new data centre, with a further five year extension signed on 2 July 2010. Approval of preliminary acquisition plan 30 June 2010. Conceptual design RFQTS released 30 June 2010. There is a late 2013 or early 2014 target to realise the vision of reducing to under 10 data centre facilities.

Strategic Imperative	Initiative	Description	Planned implementation date	Current status
	Next Generation Desktop	This initiative aims to deliver a single desktop utilising a thin client architecture supported by a consolidated and centralised data centre infrastructure environment. Multiple environments across different security domains plan to be accessible via a single device on a single screen. These changes intended to result in reduced support and maintenance costs.	2011–12	Invitation to Register evaluation complete. Restricted Request For Tender planned to be released in October 2010. Proposed solution to be piloted in January 2011. Gate 0 completed in December 2010, with delivery confidence rating of Amber [issue raised in the review pose an immediate and significant risk to the effective and timely delivery of the project outcomes – however, these appear manageable if addressed promptly] The Government announced First pass approval on 6 May 2011.
	Terrestrial Communications	The intent of the Terrestrial Communications initiative is to upgrade, replace, standardise and rationalise the Defence Terrestrial Communications Network (DTCN) in order to deliver business efficiencies, lower costs in Defence's ICT activities and achieve a secure and robust ICT capability that supports war fighting and business functions.	2012–13	Industry brief April 2010. Release Invitation to Register April 2010. Complete Invitation to Register evaluation June 2010.

Strategic Imperative	Initiative	Description	Planned implementation date	Current status
Provide agreed, priority solutions	Software Licence Rationalisation	This initiatives aims to deliver Defence the ability to manage software application licences based on business need, usage, thresholds and licence reduced support costs. Existing number of software applications in Defence is approximately 3200. The industry average ranges from approximately 300 for a large bank to 1400 for a Global Energy company. The target end state for Defence is approximately 1000 software applications.	2018–19	Scoping work has commenced.

Strategic Imperative	Initiative	Description	Planned implementation date	Current status
	Infrastructure Remediation	The aim is to update and replace old infrastructure with zero infrastructure growth. Elements of ICT Infrastructure include Fleet Management Implementation Program, Russell PABX[144] upgrade and ICT hardware refresh. Defence personnel will directly benefit with improved availability and performance and the ability to add additional functionality.	2018–19	Refreshing 100% (25 610) of the PCs and 100% (17 233) of the monitors in 2009–10. Puckapunyal Base Area Remediation 60% (due for completion in Nov 2010). Enoggera Core/Transmission Switch replacement 50% (due for completion in Dec 2010). Edinburgh Core/Transmission Switch replacement, 32 Server replacements and 127 edge switch replacements Australia wide. Printer remediation business case signed off (July 2010). Printer remediation activities aim to be completed in 2010–11.

[144] PABX (Private Automatic Branch Exchange) is the internal telephone system serving a business or office.

Appendix 3: P3M3® Maturity Levels

Table A 2

P3M3® Maturity Levels

Maturity Level	Description
Level 1 – Awareness of Process	Processes are not usually documented. There are no, or only a few, process descriptions. They will generally be acknowledged, in that managers may have some recognition of the necessary activities, but actual practice is determined by events or individual preferences, and is highly subjective and variable. Processes are therefore undeveloped, although there may be a general commitment to process development in the future. Undeveloped or incomplete processes mean that the necessary activities for better practice are either not performed at all or are only partially performed. There will be little, if any, guidance or supporting documentation and even terminology may not be standardised across the organisation – e.g. business case, risk, issues, etc. may not be interpreted in the same way by all managers and team members. Level 1 organisations may have achieved a number of successful initiatives, but these are often based on key individuals' competencies rather than organisation-wide knowledge and capability. In addition, such "successes" are often achieved with budget and/or schedule overruns and, due to the lack of formality, Level 1 organisations often over-commit themselves, abandon processes during a crisis, and are unable to repeat past successes consistently. There is very little planning and executive buy-in, and process acceptance is limited.

Maturity Level	Description
Level 2 – Repeatable Process	The organisation will be able to demonstrate, by reference to particular initiatives, that basic management practices have been established – e.g. tracking expenditure and scheduling resources – and that processes are developing. There are key individuals who can demonstrate a successful track record and that, through them, the organisation is capable of repeating earlier successes in the future. Process discipline is unlikely to be rigorous, but where it does exist, initiatives are performed and managed according to their documented plans, e.g. project status and delivery will be visible to management at defined points, such as on reaching major milestones. Top management will be taking the lead on a number of the initiatives but there may be inconsistency in the levels of engagement and performance. Basic generic training is likely to have been delivered to key staff. There is still a significant risk of exceeding cost and time estimates. Key factors that may have preconditioned the organisation to experience difficulties or failure include: inadequate measures of success; unclear responsibilities for achievement; ambiguity and inconsistency in business objectives; lack of fully integrated risk management; limited experience in change management; and inadequacies in communications strategy.

Maturity Level	Description
Level 3 – Defined Process	The management and technical processes necessary to achieve the organisational purpose will be documented, standardised and integrated to some extent with other business processes. There is likely to be process ownership and an established process group with responsibility for maintaining consistency and process improvements across the organisation. Such improvements will be planned and controlled, perhaps based on assessments, with planned development and suitable resources being committed to ensure that they are coordinated across the organisation. Top management are engaged consistently and provide active and informed support. There is likely to be an established training programme to develop the skills and knowledge of individuals so they can more readily perform their designated roles. A key aspect of quality management will be the widespread use of peer reviews of identified products, to better understand how processes can be improved and thereby eliminate possible weaknesses. A key distinction between Level 2 and Level 3 is the scope of standards, process descriptions and procedures – i.e. stated purposes, inputs, activities, roles, verification steps, outputs and acceptance criteria. This enables processes to be managed more proactively using an understanding of the interrelationships and measures of the process and products. These standard processes can be tailored to suit specific circumstances, in accordance with guidelines.
Level 4 – Managed Process	Level 4 is characterised by mature behaviour and processes that are quantitatively managed – i.e. controlled using metrics and quantitative techniques. There will be evidence of quantitative objectives for quality and process performance, and these will be used as criteria in managing processes. The measurement data collected will contribute towards the organisation's overall performance measurement framework and will be imperative in analysing the portfolio and ascertaining the current capacity and capability constraints. Top management will be committed, engaged and proactively seeking out innovative ways to achieve goals. Using process metrics, management can effectively control processes and identify ways to adjust and adapt them to particular initiatives without loss of quality. Organisations will also benefit through improved predictability of process performance.

Maturity Level	Description
Level 5 – Optimised Process	The organisation will focus on optimisation of its quantitatively managed processes to take into account changing business needs and external factors. It will anticipate future capacity demands and capability requirements to meet delivery challenges – e.g. through portfolio analysis. Top managers are seen as exemplars, reinforcing the need and potential for capability and performance improvement. It will be a learning organisation, propagating the lessons learned from past reviews. The organisation's ability to rapidly respond to changes and opportunities will be enhanced by identifying ways to accelerate and share learning. The knowledge gained by the organisation from its process and product metrics will enable it to understand causes of variation and therefore optimise its performance. The organisation will be able to show that continuous process improvement is being enabled by quantitative feedback from its embedded processes and from validating innovative ideas and technologies. There will be a robust framework addressing issues of governance, organisational controls and performance management. The organisation will be able to demonstrate strong alignment of organisational objectives with business plans, and this will be cascaded down through scoping, sponsorship, commitment, planning, resource allocation, risk management and benefits realisation.

Source: UK Office of Government Commerce, 2010, *P3M3® – Introduction and Guide to P3M3®,* Version 2.1, pp. 13–14.

Appendix 4: Strategic Reform Program Streams

Table A 3

Strategic Reform Program Streams

Savings Streams	Non-Savings Streams
Logistics	Strategy-led Planning
Reserves	Preparedness
Smart Sustainment	Capability Development
Inventory	Intelligence
Non-equipment Procurement	Output Focussed Budget Model
Workforce and Shared Services	Science and Technology
ICT	Estate
	Procurement and Sustainment (Mortimer)

Source: Department of Defence, *The Strategic Reform Program 2009: Delivering Force 2030,* 2009, pp.6–7.

Index

C

Chief Information Officer (CIO), 14, 22, 34, 37, 78

Chief Information Officer Group (CIOG), 16, 18, 34, 64

Internal Operating Model, 100

Management structure, 102

Chief of the Defence Force (CDF), 21, 34, 60, 63

D

Defence Budget Audit (DBA), 76, 78, 79

Defence ICT Program Design Manual (PDM), 43, 45, 78, 92, 119

Defence Information and Communication Technology Committee (DICTC), 17, 21, 50, 63, 70

Defence Information and Communication Technology Strategy, 14, 42, 44

Defence Information Environment (DIE), 13, 33, 36, 38, 42

Defence Information Environment Committee (DIEC), 19, 21–22, 50, 52, 55

Defence Management Review (Proust Review), 14, 42, 123, 131

I

ICT and Intelligence stream Governance Committee, 54

ICT expenditure, 18, 24, 33, 56, 78

ICT Baseline, 58, 78–79, 81

ICT project approval, 68

CIOG two-pass approval process, 71

Defence two-pass approval process, 68

Whole-of-government two-pass approval process, 68

ICT Stream Governance Committee, 63

Integrated Plan of Work (IPW), 21, 61–63, 101

Interdependencies, 25, 88

K

Key Performance Indicators (KPIs), 25, 82

P

P3M3®, 19, 26, 94

Benefits management, 104

Financial management, 107

Management control, 100

Organisational governance, 115

Resource management, 119

Risk management, 113

Stakeholder engagement, 111

Portfolio Management Office (PMO), 55, 86, 117

Portfolio prioritisation, 60

R

Review of the Australian Government's Use of ICT (Gershon Review), 68, 94, 131

Review of the Defence Accountability Framework (Black Review), 15, 22, 102, 116, 126

Risk Management, 86

S

Secretary, Department of Defence, 17, 21, 34, 49, 60, 63

Stakeholder Engagement Team(s), 21, 53, 101

Strategic Assurance Review, 64, 92, 102, 106

Strategic Reform Program (SRP), 14–15, 17, 21, 39, 41, 45, 49, 75

Performance measurement, 83

Savings target, 16, 79

Sub-portfolio committees, 53

W

White Paper, 14, 15, 38, 45, 49, 131

Workforce and Financial Management Committee (WFMC), 54, 60, 67

Series Titles

ANAO Audit Report No.1 2011–12

The Australian Defence Force's Mechanisms for Learning from Operational Activities
Department of Defence

ANAO Audit Report No.2 2011–12
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2010 Compliance)

ANAO Audit Report No.3 2011–12
Therapeutic Goods Regulation: Complementary Medicines
Department of Health and Ageing

ANAO Audit Report No.4 2011–12
Indigenous Employment in Government Service Delivery

ANAO Audit Report No.5 2011–12
Development and Implementation of Key Performance Indicators to Support the Outcomes and Programs Framework

ANAO Audit Report No.6 2011–12
Fair Work Education and Information Program
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.7 2011–12
Establishment, Implementation and Administration of the Infrastructure Employment Projects Stream of the Jobs Fund
Department of Infrastructure and Transport

ANAO Audit Report No.8 2011–12
The National Blood Authority's Management of the National Blood Supply
National Blood Authority

ANAO Audit Report No.9 2011–12
Indigenous Secondary Student Accommodation Initiatives
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.10 2011–12
Administration of the National Partnership on Early Childhood Education
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.11 2011–12
Implementation and Management of the Housing Affordability Fund
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.12 2011–12
Implementation of the National Partnership Agreement on Remote Indigenous Housing in the Northern Territory
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.13 2011–12
Tasmanian Freight Equalisation Scheme
Department of Infrastructure and Transport
Department of Human Services

ANAO Audit Report No.14 2011–12
Indigenous Protected Areas
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.15 2011–12
Risk Management in the Processing of Sea and Air Cargo Imports
Australian Customs and Border Protection Service

ANAO Audit Report No.16 2011–12
The Management of Compliance in the Small to Medium Enterprises Market
Australian Taxation Office

ANAO Audit Report No.17 2011–12
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2011

ANAO Audit Report No.18 2011–12
Information and Communications Technology Security: Management of Portable Storage Devices

Current Better Practice Guides

The following Better Practice Guides are available on the ANAO website.

Public Sector Audit Committees	Aug 2011
Human Resource Information Systems	
Risks and Controls	Mar 2011
Fraud Control in Australian Government Entities	Mar 2011
Strategic and Operational Management of Assets by Public Sector Entities –	
Delivering agreed outcomes through an efficient and optimal asset base	Sep 2010
Implementing Better Practice Grants Administration	Jun 2010
Planning and Approving Projects	
an Executive Perspective	Jun 2010
Innovation in the Public Sector	
Enabling Better Performance, Driving New Directions	Dec 2009
SAP ECC 6.0	
Security and Control	Jun 2009
Preparation of Financial Statements by Public Sector Entities	Jun 2009
Business Continuity Management	
Building resilience in public sector entities	Jun 2009
Developing and Managing Internal Budgets	Jun 2008
Agency Management of Parliamentary Workflow	May 2008
Public Sector Internal Audit	
An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions	
Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts	
Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives:	
Making implementation matter	Oct 2006
Legal Services Arrangements in Australian Government Agencies	Aug 2006