The Auditor-General
Audit Report No.11 2000–2001
Performance Audit

Knowledge System Equipment Acquisition Projects in Defence

Department of Defence

Australian National Audit Office

ISSN 1036-7632

ISBN 0 642 44297 5

Australian National
Audit Office

Canberra ACT
15 September 2000

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in the Department of Defence in accordance with the authority contained in the *Auditor-General Act 1997.* I present this report of this audit, and the accompanying brochure, to the Parliament. The report is titled *Knowledge System Equipment Acquisition Projects in Defence.*

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

Yours sincerely

P. J. Barrett
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. The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits and financial statement audits of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

Auditor-General reports are available from Government Info Shops. Recent titles are shown at the back of this report.
For further information contact:

The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone (02) 6203 7505
Fax (02) 6203 7798
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 Manager

Ray McNally

Contents

Appendices

Abbreviations

ACC	Architecture Coordination Council
ACSS	Air Command Support System
ADF	Australian Defence Force
ADFICC	ADF Intelligence Coordination Centre (Canberra)
ADHQ	Australian Defence Headquarters
AEW and C	Airborne Early Warning and Control
AHQ	Air Headquarters
AIO	Australian Imagery Organisation (Canberra)
ANAO	Australian National Audit Office
ASTJIC	Australian Theatre Joint Intelligence Centre (Sydney)
ASP 97	*Australia's Strategic Policy 1997*
BCSS	Battlefield Command Support System
BPR	Business Process Re-engineering
C^3I	Command, control, communications and intelligence
C^4ISREW	C^3I with computing, surveillance, reconnaissance and electronic warfare
CDIB	Chairman Defence Intelligence Board
CMIS	Capability Manager for Information Superiority—UK
COMAST	Commander Australian Theatre
COMNORCOM	Commander Northern Command
COSC	Chiefs of Staff Committee
CRISP	Canberra Region Information System Precinct
CSS	Command Support System
CTD	Capability and Technology Demonstrator
DAO	Defence Acquisition Organisation (now merged with SCA as DMO)
DCC	Defence Capability Committee—now known as the DCIC
DCIC	Defence Capability and Investment Committee

DIB	Defence Intelligence Board
DIE	Defence Information Environment
DIEB	Defence Information Environment Board
DIO	Defence Intelligence Organisation (Canberra)
DISG	Defence Information Systems Group
DJFHQ	Deployable Joint Force Headquarters
DMO	Defence Materiel Organisation (formerly DAO and SCA)
DND/CF	Department of National Defence and the Canadian Forces
DPA	Defence Procurement Agency—UK
DSD	Defence Signals Directorate (Canberra)
DSTO	Defence Science and Technology Organisation
EA	Evolutionary Acquisition
EW	Electronic Warfare
FEG	Force Element Group
HC^{4}ISREW	Head C^{4}ISREW
HDIS	Head Defence Information Systems (Group)
HQAC	Headquarters Air Command (Glenbrook)
HQAST	Headquarters Australian Theatre (Sydney)
HQNORCOM	Headquarters Northern Command (Darwin)
HQSCA	Headquarters Support Command Australia (Melbourne)
HQSO	Headquarters Special Operations (Sydney)
IM	Information Management
IO	Information Operations
IPT	Integrated Project Team
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JCSS	Joint Command Support System
JISS	Joint Intelligence Support System
JOA	Joint Operational Architecture
JSA	Joint Systems Architecture

JSSA	Joint Support Systems Agency—DISG
JTA	Joint Technical Architecture
LHQ	Land Headquarters (Sydney)
MGI	Military Geo-spatial Information or Military Geographic Information
MHQ	Maritime Headquarters (Sydney)
NATO	North American Treaty Organisation
NORAD	North American Aerospace Defense Command
NORCOM	Northern Command
RMA	Revolution in Military Affairs
SCA	Support Command Australia
SDR	Strategic Defence Review
SFCSS	Special Forces Command Support Systems
UK	United Kingdom
UK MoD	UK Ministry of Defence
UN	United Nations
USA	United States of America
VCDF	Vice Chief of the Defence Force

See also Glossary

Summary and Recommendations

Summary

Background

1. The Defence mission is *to prevent or defeat the use of armed force against Australia and its interests*. This calls for effective command and control of the Australian Defence Force (ADF). ADF command and control depend on a wide range of information and administrative system technologies to assist the analysis of requirements, allocation of resources, integration of effort, management of logistics and coordination and monitoring of force behaviour.

2. The Government's national defence policy identifies the highest capability development priority as 'the knowledge edge' to allow Australia to use its relatively small force to maximum effectiveness. The knowledge edge depends on effective exploitation of human intellectual capital, as well as on command and control structures and decision processes coupled with information, information systems and associated infrastructure. Defence's military and administrative information systems combine to form the Defence Information Environment (DIE) and are known as *knowledge systems*.

3. Defence is pursuing the knowledge edge by investing extensively in knowledge system acquisition projects. Approved and planned projects that will have a substantial impact on the DIE have a total estimated value of almost $8.5 billion.

4. The audit objective was to assess Defence's arrangements for higher-level management of its knowledge system projects and to provide a degree of assurance about its ongoing capacity for efficient and cost-effective management in this area. A principal aim was to formulate, where circumstances required it, practical recommendations that would enhance Defence's management of those projects and their coherence with Defence's other knowledge systems. The focus of the audit was on the opportunities for Defence to adopt a much more coherent and integrated approach to knowledge systems management prospectively rather than on emphasising current system compatibility issues.

Overall conclusion

5. Defence's new arrangements for a Chief Knowledge Officer, supported by revised governance and accountability arrangements, aim to achieve a holistic approach to knowledge edge development. This

will help ensure that Defence's numerous separate knowledge systems provide their maximum contribution to ADF capability, particularly by maximising synergies and improving coherence and integration between those systems.

6. Defence is aware of the need to exploit its knowledge systems and is working to achieve improvements. In particular, the Vice Chief of the Defence Force's Owner Support Executive is working to take the lead in knowledge system program management so that Defence's information environment may be developed as a coherent whole. However, knowledge edge development is a demanding area of defence capability development. Institutional, organisational and procedural difficulties in Defence remain and these need to be overcome if the above aims are to be achieved.

7. Defence's total knowledge system consists of a vast 'system of systems'. It is necessarily decentralised across all Defence outputs but it needs centralised management to preserve system integrity and maximise synergies. Defence's new approach is to regard the knowledge system as a virtual capability and to manage it accordingly. This seems to be a sound approach, since it provides the required focused responsibility, accountability and authority for formulating and adopting strategies and plans for knowledge system policy and capability development.

8. The goal of building a knowledge system based on a coherent architectural framework is necessarily long-term and challenging, given the rapid advances in technology, wide-ranging tasks that the ADF may be called on to perform and Defence's evolving organisational relationships and business processes.

9. The Chief Knowledge Officer and his staff have much to do to bring the Defence information environment under adequate managerial control. Many knowledge system elements now in service were selected on the basis of individual functionality and not on the basis of their architectural compliance with the broader system of systems.

10. The program management and architectural goals are worthwhile due to the many substantial benefits that knowledge system coherence and integration will provide from Defence's military and business process perspectives. Critical success factors relate to the degree of program management discipline that can be applied to knowledge edge development and maintenance. The most substantial risks to knowledge system projects may be those associated with development and retention of skilled individuals needed in all parts of the Defence information environment.

Key Findings

11. The task of improving synergies and coherency between Defence's knowledge systems requires the Chief Knowledge Officer and the Knowledge Staff, with the backing of the Defence Information Environment Board, to examine all significant equipment and application projects, approved and planned, for their contribution to the DIE and their dependence on it. The objective is to have the ability to move information readily to any area in the DIE that might have a legitimate need for it and to apply required information to a particular purpose.

12. The Chief Knowledge Officer is establishing the processes needed for effective program management of the $4.5 billion in knowledge system projects that he sponsors. Subject to some caveats, processes to achieve inter-operability between these projects are now being put in place. The Chief Knowledge Officer's staff are confident of achieving improved coherency between these projects. The importance of that achievement should not be underestimated and, if successful, it should result in much improved knowledge system capability.

13. The situation is much less clear for the many other projects, estimated to cost some $4 billion, that will contribute to, or depend on, the DIE. It is not clear that processes are sufficiently robust to allow the Chief Knowledge Officer to scrutinise these projects and, where appropriate, to challenge a perceived lack of coherency between the project and the DIE.

14. From an information coherency perspective, Defence's business systems are the area of greatest concern to the Chief Knowledge Officer. Business and other administrative systems assist in financial, personnel, logistics and information management functions. Defence uses about 150 logistics systems and many personnel and administrative information management systems. This is a result of business processes that allowed managers to acquire information systems to satisfy their individual functional requirements. As a consequence, the degree of commonality and ability to exchange information between these systems is limited.

15. During acquisition, many technical decisions are taken that can, and do, seriously affect DIE integrity and coherence. The UK Ministry of Defence recently addressed the need for formal management of integration issues during acquisition by establishing an Integration Authority in its Defence Procurement Agency. The Integration Authority seeks to maintain technical visibility of all relevant projects under procurement and to bring to attention any developments that could

adversely affect information coherency. Defence could adopt a similar arrangement by establishing a close working relationship between an integration authority and the Chief Knowledge Officer.

16. An effective and consistently applied standard project management method[1] is an important foundation for good program management. Defence is adopting a Standard Project Management Method (SPMM) for some 200 major equipment acquisition projects. However, progress to date indicates that not all acquisition projects will be converted to SPMM until 2001. Moreover, there appear to be problems in achieving effective application of the SPMM. As at April 2000, for example, there were 64 acquisition projects subject to the SPMM but only two of these were assessed as controlling their projects well using the SPMM. Some action may be warranted not only to ensure that SPMM in Defence does not come in too many variations, but also to remove any confusion about the role of SPMM and any associated Project Boards, Integrated Product Teams, Integrated Acquisition Teams and Integrated Project Teams.

17. The Defence Science and Technology Organisation (DSTO) believes that the Evolutionary Acquisition (EA)[2] project management technique can deliver functionality sooner than other acquisition methods, and that it should be adopted for a range of projects, including software-intensive projects and other projects subject to rapid technological change. DSTO has found that, even though EA has become an approved acquisition strategy in Defence, there is a widespread view in Defence that EA guidance is either lacking or poorly developed and that EA's full potential is not being realised.

18. The military and civilian workforce that supports the DIE is spread across a wide range of projects and endeavours. Shortages of skills in one area are addressed by denying essential skills to another. The DIE is vulnerable to shortages in staff with the appropriate skills and experience. Statistics indicate that the three Services encounter difficulties in recruiting and retaining the skilled personnel needed to support the DIE.

19. The ANAO made seven recommendations designed to address these issues. Defence agreed to the recommendations, one with qualification. The Secretary of the Department has indicated that aspects of the report would serve as action statements in Defence in this area.

---

[1] Predefined set of concepts and project management processes that are the minimum requirements of a properly run and managed project.

[2] See Glossary.

Recommendations

Set out below are the ANAO's recommendations, with report paragraph references and an indication of Defence's response.

Recommendation No.1 Para. 4.5

The ANAO *recommends* that, to assist the formulation and adoption of strategies and plans that promote coherence among information systems, Defence give priority to articulating an architecture (or architectures) for the future Defence Information Environment.

Defence response: Agree.

Recommendation No.2 Para. 4.16

The ANAO *recommends* that Defence develop more-disciplined program management processes by which the Chief Knowledge Officer can scrutinise military projects not sponsored by him and, when appropriate, require improvements in the coherency between those projects and the Defence Information Environment.

Defence response: Agree.

Recommendation No.3 Para. 4.25

The ANAO *recommends* that Defence develop formal transparent processes to allow the Chief Knowledge Officer to scrutinise the future development of Defence's administrative systems and assess their coherency with the Defence Information Environment.

Defence response: Agree.

Recommendation No.4 Para. 4.35

The ANAO *recommends* that Defence:

a) clarify the Chief Knowledge Officer's role as the customer for acquisition projects that he sponsors; and

b) consider the costs and benefits of establishing an Integration Authority, along the lines of that established in the UK Defence Procurement Agency.

Defence response: Agree.

Recommendation No.5 Para. 4.42

The ANAO *recommends* that Defence carefully monitor its adoption of the Standard Project Management Method (SPMM) to ensure that core and essential elements have a high degree of consistency across Defence.

Defence response: Agree.

Recommendation No.6 Para. 4.48

The ANAO *recommends* that Defence assess the priority to be given to exploiting the advantages of Evolutionary Acquisition methods, particularly for projects with a significant impact on the Defence Information Environment, and take the requisite action.

Defence response: Agree.

Recommendation No.7 Para. 4.53

The ANAO *recommends* that Defence undertake formal workforce planning and assessments of the Defence Information Environment workforce to ensure that training, postings, career prospects and professional development are carefully planned and that a holistic view, at least in a strategic sense, is taken in relation to these matters.

Defence response: Agree, with qualification.

Audit Findings and Conclusions

1. Knowledge System Equipment Acquisition Projects

This chapter provides an overview of Defence's knowledge system projects and recent changes in the way these projects are grouped and managed. It also sets out the audit objective, scope and method.

Introduction

1.1 The Defence[3] mission is *to prevent or defeat the use of armed force against Australia and its interests*. In 1994 the then Vice Chief of the Defence Force (VCDF) stated:

> *The nature of warfare is changing. In the three components of warfare—the application of brute force, the smart application of modern weapons systems, and the availability of knowledge—the trend is towards the smart end of the spectrum, away from brute force. And you can see that exhibited very strongly in the Gulf War.*[4]

The 1994 Defence White Paper gave priority to:

> *…developing the Australian Defence Force as an integrated whole, including command arrangements and doctrine at the operational level; and*
>
> *…carefully identifying areas and capabilities in which we need to maintain a high degree of excellence, in particular, command, control and communications.*[5]

The present Government's Defence policy statement (1997) identified the highest capability development priority as:

> *…the 'knowledge edge'; that is, the effective exploitation of information technologies to allow us to use our relatively small force to maximum effectiveness.*[6]

---

3 'Defence' comprises the Department of Defence and the Australian Defence Force (Navy, Army and Air Force).

4 Lieutenant General J.S. Baker AO, Vice Chief of the Defence Force, *Opening Address, Command and Control Towards 2005 Seminar*, Canberra, 9–10 November 1994. Department of Defence, Dev 94–3509 DGFD (J) 446/95, 28 March 1994. [Classified internal report.]

5 Department of Defence, *Defending Australia, Defence White Paper 1994*, AGPS Canberra, November 1994, p.34.

6 Department of Defence, *Australia's Strategic Policy*, 1997, p.56.

In 1998 Defence identified a need to:

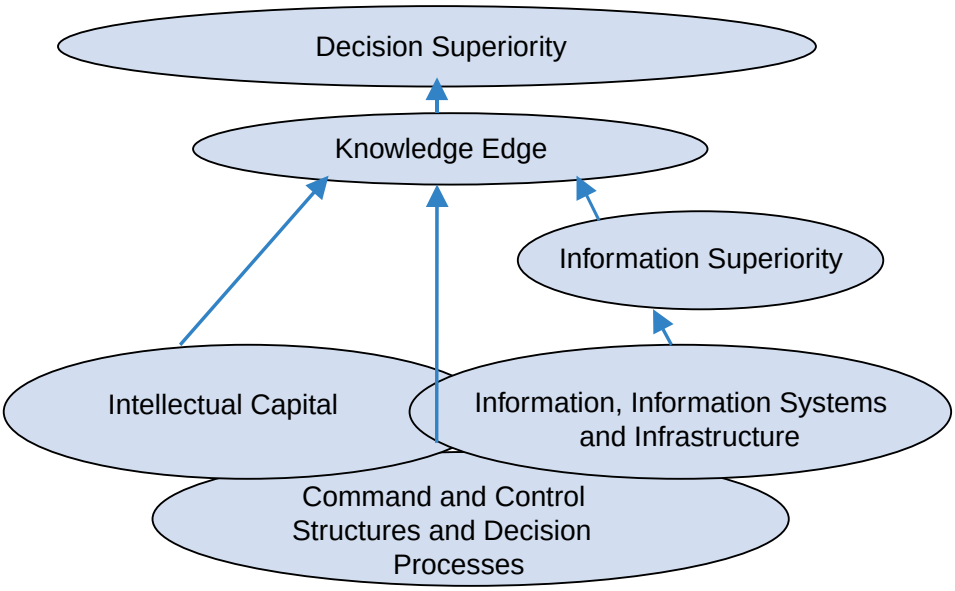
> *... take advantage of technological advances and other trends, particularly in integrating the command, control, communication and intelligence systems that underpin our knowledge edge.*[7]

1.2 Defence's increasing emphasis on the knowledge edge, and the resulting improvements in decision-making, has led it to better define the way it manages its knowledge. The knowledge edge that leads to superior decision-making is based on a hierarchy of understanding. At the lowest level are data related to facts or numbers. At the middle level is information derived from the collation of data and any associations that may flow from that. The highest level is intelligence or knowledge that results from uniquely human cognitive process of applying reason, intuition and perception to data and information.

1.3 Thus an organisation's knowledge edge is resident in the minds of its people, and, where possible, stored in information systems. Its decision superiority is influenced by personnel skills and the organisation's ability to gather and process information for accurate and timely presentation to decision-makers. Defence has grouped the components of its knowledge edge as shown in Figure 1.

Figure 1

Decision Superiority and the Knowledge Edge



Source: adapted by the ANAO from Defence records

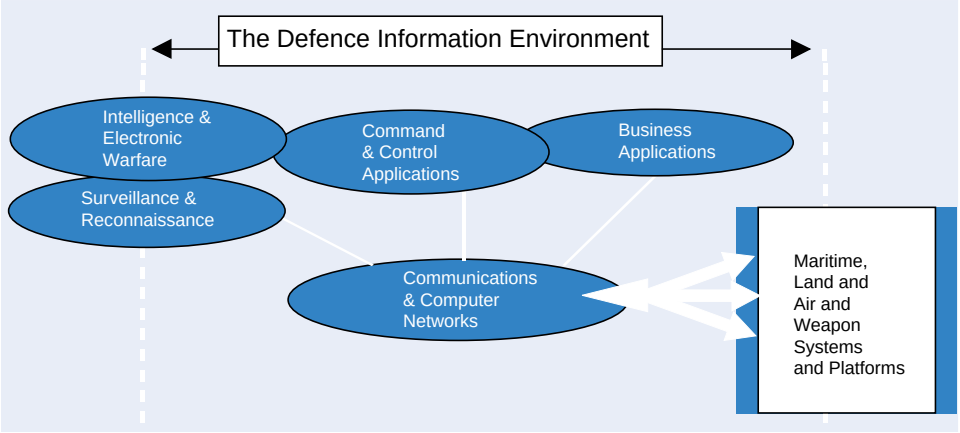
[7] Department of Defence *Defence—Our Priorities*, November 1998, p.6.

The knowledge edge and the Revolution in Military Affairs

1.4 The knowledge edge depends on a combination of military and administrative information systems that collectively form the Defence Information Environment (DIE). Figure 2 illustrates the way that the DIE, shown as interconnected ovals, relates to the maritime, land and air capabilities of the Australian Defence Force (ADF).

Figure 2

The Defence Information Environment



Source: Prepared by the ANAO from Defence records

1.5 The DIE's purpose, as expressed in the April 1999 DIE Strategic Plan, is to contribute to the success of ADF operations and campaigns by:

- ensuring commanders and staff have access to the information needed to achieve decision superiority;
- contributing decisively to the knowledge edge of capability; and
- contributing to the operation of the Defence organisation as a high-performing, single enterprise.

1.6 The knowledge edge is a central feature of the 'Revolution in Military Affairs' (RMA). The RMA is based on technology advances that enable higher levels of precision in military operations through new technologies, including improvements in command and control systems; intelligence, surveillance, reconnaissance and electronic warfare systems; administrative systems; and information processing. However, the RMA goes beyond improvements in various individual systems. It seeks increased synergy through better coherence and integration of separate sensors, weapon systems, military platforms and administrative systems.

C^4ISREW Staff

1.7 On 1 July 1999 Defence established a Division in Defence Headquarters, and under VCDF, with the title C^4ISREW Staff and headed by Head C^4ISREW (HC^4ISREW). This was in recognition of the knowledge edge significance of C^3I systems and their close interaction with combat information systems and sensors. The acronym C^4ISREW stands for command, control, communications, computers, intelligence, surveillance, reconnaissance, and electronic warfare. HC^4ISREW was given program management responsibility for policy direction and capability development of the DIE.

Chief Knowledge Officer, the Knowledge Staff and knowledge systems

1.8 On 23 June 2000 Defence announced major changes to its higher-level governance and accountability framework. The detail is to be completed in October 2000. VCDF and the C^4ISREW Staff are now part of an 'Owner Support Executive' and the titles of HC^4ISREW and his staff have been simplified to Chief Knowledge Officer and the Knowledge Staff. In line with these changes, this report uses the generic term *knowledge systems* interchangeably with C^4ISREW to describe the numerous systems that come within the area of interest of the Chief Knowledge Officer and the Knowledge Staff. Also, the titles Chief Knowledge Officer and Knowledge Staff are used throughout this report in place of the former titles of HC^4ISREW and C^4ISREW Staff.

Taking stock of information system projects

1.9 Defence is pursuing the knowledge edge by investing extensively in knowledge projects. Prior to the Defence Reform Program (introduced in 1997), Defence's command, control and communications (C^3) and information technology (IT) investment strategies favoured the needs of individual Defence groups or one of the three Services, with the result that little was done to track and manage knowledge systems centrally. This situation improved in recent years with respect to ADF-wide projects such as the Joint Command Support System (JCSS). Defence is now taking stock of all its current and proposed projects relevant to its information environment.

1.10 Approved and planned military projects, that will have a substantial impact on its information environment, have a total estimated value of almost $8.5 billion. This comprises $4.5 billion in new information system projects directly sponsored by the Chief Knowledge Officer (listed in Appendix 1) and some $4 billion in projects sponsored elsewhere in Defence. The latter group includes the proposed $2.2 billion acquisition

of air defence Airborne Early Warning and Control aircraft.[8] Intelligence, surveillance and reconnaissance systems (ISR) and military geo-spatial information systems (MGI) projects account for some 60 per cent of the total of $8.5 billion.[9]

1.11 There are also a significant number of administrative systems that do, or will, contribute significantly to Defence's information environment. There is little information collated centrally about these systems because, for decades, Defence's various functional groups decided on, and funded, their administrative systems to suit their own purposes. For example, Defence records indicate there are some 150 different systems in the logistics organisation alone.

The audit

Background

1.12 The ANAO's *Performance Audit Work Program 1999–2000* provided for an audit in Defence of a group of projects known as C³I—command, control, communications and intelligence. C³I systems provide strategic and tactical command, control and intelligence data during military operations and training, and are significant in helping Defence achieve its mission.

1.13 Because of later developments, summarised in paragraphs 1.7 and 1.8, and the subsequent emphasis on the knowledge edge, the ANAO widened the scope of its audit to embrace Defence's management of the acquisition project aspects of its knowledge edge development.

Audit objective and scope

1.14 The audit objective was to assess Defence's arrangements for higher-level management of its knowledge system projects and to provide a degree of assurance about its ongoing capacity for efficient and cost-effective management in this area. A principal aim was to formulate, where circumstances required it, practical recommendations that would enhance Defence's management of those projects and their coherence with Defence's other knowledge systems.

1.15 Audit Report No.13 1999–2000 *Management of Major Equipment Acquisition Projects—Department of Defence* dealt with higher-level project management issues in detail. This audit did not revisit those issues—

---

[8] The approved project cost is as shown in *DAO Black Book*, AIR 5077, 17 November 1998.

[9] DGC3I, *Defence Information Environment Audit Interim Report*, 27 April 1999, Enclosure 1, p.4 (classified internal report). The Defence Information Environment audit was not complete at the time of the ANAO audit.

apart from reporting on selected business process re-engineering relevant to knowledge system management. Nor did the audit cover the intellectual capital elements of the knowledge edge such as, personnel training and professional mastery, team cohesion and morale, leadership and command authority, and decision culture.

1.16 The focus of the audit was on the opportunities for Defence to adopt a much more coherent and integrated approach to knowledge systems management prospectively rather than on emphasising current system compatibility issues. It therefore focused on the need for:

- a corporate governance system capable of ensuring the achievement of the organisation's objectives in the area of C[4]ISREW equipment acquisition projects;
- business processes that address areas of difficulty in knowledge edge related program management and equipment acquisition project management; and
- continued availability of suitably skilled personnel.

Audit criteria were derived from these desired attributes.

1.17 The audit focused particularly on the strategic-level management of equipment acquisition projects that relate to the development of Defence's knowledge edge. In Figure 1 these projects appear within the 'information, information systems and infrastructure' oval. They include a wide range of military information and administrative system technologies that assist Defence personnel to analyse requirements, allocate resources, integrate effort, manage logistics and coordinate and monitor of force behaviour.

1.18 The Defence Information Systems Group (DISG), mentioned throughout this report, is the Defence Enabling Executive responsible for developing and operating many of Defence's administrative information systems and maintaining some command support systems.

1.19 During this audit, Defence commissioned an information technology management firm to review the DISG operations in terms of:

- infrastructure technology choices;
- acquisition policies, procedures and processes;
- capability development processes as they relate to DISG;
- DISG's management and operational structure;
- DISG's interfaces with client groups and other organisations; and
- the change management strategies implemented.[10]

---

[10] Defence Information Systems, *External Review of DISG*, ASCM CM 40/00, 23 March 2000.

1.20 The ANAO did not duplicate this work. However, the results of the review were not available at the time of audit fieldwork.

Audit method

1.21 A preliminary study began in October 1999 and proceeded to an audit in December 1999. The audit encompassed fieldwork in Defence's Offices in Canberra and visits to ADF centres in Sydney and Darwin. The audit involved discussions and review of documents. The ANAO interviewed a range of senior executives and managers involved in C[4]ISREW system development in Australia, the United Kingdom, United States and Canada. Audit discussion papers setting out preliminary findings and conclusions were provided to Defence for comment throughout the audit.

1.22 Managerial complexity associated with knowledge edge related acquisition projects, combined with corporate governance and business changes now under way in Defence, heightened the need for cooperation between the audit team and the Knowledge Staff. The audit benefited from extensive interaction with Knowledge Staff and from their liaison role with other parts of the C[4]ISREW community. In particular the ANAO thanks Brigadier Tim McKenna, Group Captain Brett Biddington, Lieutenant Colonel Ewart Challis and Commander David Johnston RAN for their positive assistance.

1.23 The audit team comprised the audit manager and Mr Tom Hayes AO, a consultant engaged by the ANAO to assist on the audit with his experience in Defence acquisition management and wider public-sector management. The proposed report of the audit was provided to Defence in August 2000 for comment. The final report was prepared having regard to Defence's comments. The audit was conducted in conformance with ANAO auditing standards and cost $331 000.

1.24 The ANAO made seven recommendations designed to address these issues. Defence agreed to the recommendations, one with qualification. After the proposed report was provided to Defence, the Secretary of the Department of Defence gave an address entitled *In Search of the Knowledge Edge—The Management Component*, which indicated that aspects of the audit report would serve as action statements in Defence in this area. His address is at Appendix 8.

Report structure

1.25 The remainder of this report is organised in three chapters, as follows:

- Chapter 2 discusses knowledge edge related corporate governance, strategy and development.
- Chapter 3 discusses how knowledge system outputs appear across Defence's outputs.
- Chapter 4 brings together the ANAO's assessment of seven key management issues concerning knowledge system projects in Defence and makes recommendations.

2. Knowledge Edge Governance, Strategy and Development

This chapter describes the organisational changes and business processes Defence has applied to the tasks involved in developing its knowledge systems.

Introduction

2.1 Data and information are essential to all forms of defence force activity. Defence's knowledge system 'continuum' stretches from the Department's business administration and logistics information systems to the ADF's front-line combat information systems and sensors.

2.2 The ability to establish and exploit a knowledge edge in military conflict depends on having data collection and information systems that have a range of desirable characteristics. Data and information need to be developed and shared in a coherent and integrated manner with all areas of the organisation with legitimate needs for them. Part of the drive for better coherency between information systems comes from a view that Defence information systems already collect considerable data potentially useful to various groups in the organisation but often inaccessible for reasons of incompatibility of systems. This is particularly so in respect of data in Defence's various administrative systems. Much of that data is collected at considerable cost but accessible only by personnel with detailed knowledge of, and experience with, a particular system and application.[11]

2.3 In 1998 Defence identified a need to *take advantage of technological advances and other trends, particularly in integrating the command, control, communication and intelligence systems that underpin our knowledge edge.*[12] Defence is seeking to achieve this objective through revised organisational arrangements and new approaches to knowledge system development and by reforming its equipment acquisition methods.

---

[11] For example, Audit Report No.26 1999–00 *Army Individual Readiness Notice* set out the ANAO's reservations about Army's access to reliable data on soldiers' individual readiness.

[12] Department of Defence *Defence—Our Priorities*, November 1998, p.6.

Corporate governance of the Defence information environment

2.4 In November 1998 Defence established the Defence Information Environment Board (DIEB) with the intention of designing, implementing and managing the Defence information environment (DIE) in a holistic manner. The DIEB's functions and the DIE's stakeholders are listed in Appendix 2. Defence defines its DIE as a combination of:

- C^4ISREW capability and Defence business and operational support system capability;
- communications infrastructure;
- architecture and design;
- information assurance;
- personnel aspects;
- interoperability;
- research and development, including liaison with industry; and
- knowledge system modelling and simulation capability.[13]

2.5 In June 1999 the Australian Defence Headquarters staff was re-formed. The position of Head C^4ISREW was created and made responsible for providing C^4ISREW policy direction and capability development. This arrangement strengthened the focus on knowledge edge development by bringing together, from within ADHQ and elsewhere in Defence, a single group of staff responsible for the policy direction and capability development for the Defence information environment. Also in 1999, the Head of Defence Information Systems (HDIS) became Defence's Chief Information Officer (CIO) under ADHQ's Deputy Secretary Resources and Management.

2.6 In October 1999, the Minister for Defence announced the establishment of the Defence Intelligence Board (DIB).[14] The DIB aims to manage better Defence's intelligence resources and to maximise intelligence outputs. The DIB's Chairman is accountable for its performance and responsible for managing staff allocated to intelligence and for overseeing and coordinating the Defence intelligence community. The DIB directs the overall planning and management of the Defence Intelligence Organisation (DIO), Defence Signals Directorate (DSD) and the Australian Imagery Organisation (AIO).

---

[13] Department of Defence, *The Knowledge Staff Business Plan 1 July 2000 to 30 June 2001*, 16 September 1999, p.3.

[14] Minister for Defence, *New Defence Intelligence Arrangements*, MIN321/99, 28 October 1999.

2.7 On 23 June 2000, Defence announced major changes to its higher-level governance and accountability framework. Actual details are to be announced in October 2000. Defence is seeking to improve its governance capabilities by setting clearer direction, and ensuring progress is made, toward long-term goals. VCDF and the former C4ISREW organisation are now part of an 'Owner Support Executive.' The Owner Support Executives are to *support the governance role, and are focused on Government and its role of owner of the enterprise rather than as a customer.*[15] This makes the Chief Knowledge Officer the owner's chief representative on knowledge system development matters in terms of setting direction and ensuring proper progress is achieved.

Changes to general approach to knowledge system development

2.8 A significant knowledge edge initiative was to bring together, in one organisation under the Head of C4ISREW, program management responsibility for policy direction and capability development of the Defence information environment, including:

- the architecture of the DIE and interoperability of DIE systems;
- command and control (C^2), communications and computers; intelligence, surveillance and reconnaissance (ISR); electronic warfare (EW); and information operations (IO);
- military geographic information (MGI) and sponsorship of the MGI function across Defence;
- personnel and training issues for DIE operators and users;
- corporate applications and infrastructure including logistic support information;
- knowledge management;
- interoperability of military C^2, Defence business and civilian systems to support electronic business; and
- monitoring and oversight of C4ISREW aspects of other approved projects in the acquisition phase to ensure compliance with the architecture of the DIE.

[15] *Defence Governance and Accountability*, Presentation by Dr Allan Hawke at the Senior Leadership Recall Day, 23 June 2000, p.4.

2.9 The Chief Knowledge Officer and the Knowledge Staff's key function was described in July 1999, by the then VCDF, as follows:

> *The Defence Information Environment, or C4ISREW, is a system of systems: including command and control, communications, computers, Intelligence, Reconnaissance, and Electronic Warfare. It should be a virtual capability, delivering systems that provide superior situation awareness for commanders to exploit the Knowledge Edge…*
>
> *…But, and this is key, Head C4ISREW will lead the team that stitches this capability together, working closely with the senior commanders and staff of all the Capability Output Managers and Enabling Output Managers...* [16]

Knowledge edge development strategies and plans

2.10 Formulating and adopting strategies and plans to manage all defence knowledge edge issues in a coherent and integrated way is a challenging task, even for highly developed nations such as the UK, USA and Canada. Lessons learnt from their experience are outlined in Appendix 3.

2.11 One key lesson learnt is the need for a clear architectural approach to knowledge system development strategies and plans. The UK Ministry of Defence's Capability Manager for Information Superiority (CMIS) is tasked with selecting specific equipment concepts to meet information superiority capability gaps. The CMIS team use architectures that reduce complexity, increase flexibility and improve co-operation between people, processes and technology. The CMIS organisation uses two architectures: a business architecture that includes military operations, and an information and communication technology services architecture. According to the CMIS:

> *The pace of business change and technology advance is now so rapid that any attempt to produce, endorse or implement any form of strategy is considered questionable, unless that strategy concentrates only on these aspects that are enduring and which transcend such changes. A properly formulated architecture provides the means to capture these enduring aspects whilst providing a structured framework within which the more rapidly changing elements can be evolved and updated as a coherent whole.*[17]

---

[16] Vice Chief of the Defence Force, *Open Letter to Australian Defence Headquarters Capability Staff*, 7 July 1999, Enclosure p..3.

[17] 'Architecture' is used in its normal English sense, that is to describe 'a special method or style of structure and ornamentation' Oxford English Dictionary, or 'a unifying or coherent form or structure' Websters Dictionary. UK Ministry of Defence, Information Superiority Capability Manager, *Delivering Information Superiority—Architectures for Information Coherence in support of the Modern Battlespace and Information Age Government*, issue 1, 17 March 2000, pp. 5 and 8.

2.12 The US Department of Defense has also adopted an architectural framework based on operations, systems and technical architectures. The Canadian Department of National Defence and the Canadian Forces are also developing an information management architecture. These are also discussed in Appendix 3.

2.13 In 1998, the then Australian Defence Headquarters (ADHQ), with assistance from Defence Science and Technology Organisation (DSTO), began work on developing an architectural framework and joint 'system of systems' approach to knowledge system capability development. The framework now comprises three hierarchical levels as follows:

- a top-level operational architecture based on concepts of operations, including the way the ADF conducts and commands operations as a joint force and conducts defence business as a single enterprise;
- a mid-level systems architecture that influences the way all Defence's communication and computing systems may be integrated and developed to achieve the ADF's operational needs within the limits of technology; and
- a lower-level technical architecture that influences C^3I interoperability standards in the ADF and allied commands, as well as the way Defence can move to a common operating environment that ranges from desk-top networked personal computers to combat systems deployed in the field.

2.14 This framework involves the Knowledge Staff, DSTO and others working together on knowledge system simulation and experimentation. DSTO has invested some $60 million in capability and technology demonstrator (CTD) programs that help define requirements for knowledge and other systems prior to any acquisition action.

2.15 The architectures work is intended to provide for better outcomes in terms of strategic direction and program management. It emphasises the need to ensure data, information and business processes are compatible, complementary, consistent and best suited to the organisation's operations. The overall aim of the architectures approach is to assist in ensuring that those responsible *plan and operate the DIE on a whole of life basis to an approved budget and within a cohesive enterprise wide context*.[18]

---

[18] Department of Defence, *Knowledge Staff, Business Plan, 1 July 2000 to 30 June 2001*, p.4.

2.16 In May 2000 ADHQ engaged a firm to complement and extend the Defence information environment architectural framework. The overall aim is to develop knowledge edge development strategies and plans by basing them on the above three-level architecture framework. ADHQ is developing the operational level of the architecture first, because of its primacy in the organisation's business processes, and its scope for driving the formation of the systems and technical elements.

2.17 However, the Knowledge Staff recognise that the three architectural elements interact, particularly when technological advances warrant changes to business processes and system designs. For this reason the Chief Knowledge Officer, who is responsible for the knowledge system's operational and systems part of the architecture, will need to work closely with the Chief Information Officer (CIO—HDIS). The CIO is responsible for the technical element of the architecture in terms of compliance with technical standards and information systems service delivery. They will also need to work closely with the Chief Finance Officer, who is responsible for the financial elements of Defence's business strategy. This also means that the architectural work needs to be well focused and have sufficient priority in order for it to cope with business process changes and technological advances.

2.18 The *Knowledge Staff Business Plan* outlines the Knowledge Staff organisational structure, vision, goals, work priorities and links with Defence's balanced score card performance reporting system. The plan is linked to the knowledge system architectural framework in terms of the future development of an integrated communications network, that includes Defence's fixed and mobile communication systems; and a national integrated intelligence, surveillance, reconnaissance and electronic warfare system (or system of systems).[19]

Acquisition methods for knowledge edge systems

2.19 Modern military forces seek to achieve 'digitisation of the battlespace', which calls for increased use of digital communications and computer systems in all areas of military endeavour. This technological development has merged previously separate areas of computing and communications. However, this has also created more risk of serious incompatibilities between various knowledge systems. Improvements in interoperability between systems in a nation's defence force are now said to be more important than fielding new systems.

2.20 Part of the difficulty in managing advances in technology is that

---

[19] Department of Defence, *The Knowledge Staff Business Plan 1July 2000—30 June 2001*, pp.4,5.

advances in some areas are more rapid than in others. Keeping reasonably abreast of the best technology in individual areas means that military knowledge systems are never fully interoperable. But this should not allow separate groups to pursue what is technologically attractive in a local domain without careful consideration of its impact on the whole information environment.

2.21 The technical complexity of Defence's knowledge system requires program management, project management, systems engineering and contracting practices that are flexible and allow controlled evolution and iteration in defining user requirements and in systems engineering. The required flexibility is available in Defence's:

- 'evolutionary acquisition' processes;[20]
- military system development standards that contain iterative development methodologies;[21] and
- Standard Project Management Method (SPMM), which allows for greater stakeholder involvement in the oversight and direction of acquisition project management.

2.22 However, these place high demands on program and project management skills within Defence's individual project 'supplier' and 'customer' organisations. Organisational and procedural difficulties remain and these need to be overcome by changes in corporate governance, architectural frameworks, business processes and personnel training such as those discussed in this Chapter and in Chapter 4. As well, project evolution and iteration are sometimes costly in time and effort. Care needs to be taken that project management and reporting practices are not unduly protracted or redundant.[22]

2.23 Additional flexibility may be found in a range of contracting practices under review by Defence Materiel Organisation (DMO), which was formed on 1 July 2000 by the merger of the Defence Acquisition Organisation (DAO) and Support Command Australia (SCA). DMO is considering the need for contracts to be better tailored to the systems engineering aspects of particular projects.[23] These include revised incentive-based contracting, the use of commercial or private sector

---

[20] See Glossary.

[21] Audit Report No. 28, 1995–96 *Jindalee Operational Radar Network Project—Department of Defence*, p.34.

[22] Lessons regarding project management and reporting practices applicable to iterative projects are discussed in Department of Defence, Management Audit Branch *Final Audit Report Joint Project 2030—Joint Command Support Environment* April 1998, p.18.

[23] Blake Dawson Waldron *Report on Financial Aspects of Contract Terms and Conditions* August 1999, pp.70–71 [report produced for the Department of Defence].

standards and revised specification standards. As with other types of contracting, it is sound practice to avoid over-specification of requirements that may put at risk consideration of alternative ways of providing the required outputs and outcomes.

Conclusion

2.24 Defence's new Chief Knowledge Officer arrangement, supported by governance and accountability changes and architectural frameworks, aims to achieve a holistic approach to knowledge system development. This will help ensure that each knowledge system project makes its maximum contribution to ADF capability, particularly by maximising the synergy between various elements through improved coherence and integration.

2.25 Defence Headquarters, the Services, DSTO, DISG and DMO are working together to achieve improvements. In particular, VCDF's Owner Support Executive is working to take the lead in knowledge system program management so that Defence's knowledge systems may be developed as a coherent whole. However, this is a demanding area of defence capability development, and there is much still to be done at the organisational and procedural levels. The architectures framework, combined with the new corporate governance and program management, offers significant improvements over earlier approaches to knowledge edge policy and development.

3. Knowledge System Outputs

Elements of Defence's knowledge system appear as part of Defence's Output structure. Many individual systems are networked together to form a 'system of systems' that aims to exploit the knowledge edge.

Introduction

3.1 This chapter deals with those elements of the knowledge system that are in operational service and hence appear as part of Defence's Output structure. During the audit, Defence announced changes to organisational structures needed to manage five 'Outputs', 28 'sub-outputs' and 35 'sub-sub-outputs'.[24]

3.2 Appendix 4 shows the Defence Information Environment from a Defence outputs viewpoint and the distribution of knowledge system elements among those outputs. Appendix 5 lists all Defence's outputs.

Knowledge system output management

3.3 Defence does not have an individual Output Manager responsible for the overall knowledge system capabilities now in service. C^3I systems in the past were largely confined to supporting single-Service activities and were far less complex than those now in use and being developed. Also, the Defence intelligence organisations developed their own specialised intelligence systems, as did the Services for their own specialised surveillance, reconnaissance and electronic warfare systems.

3.4 Output management of knowledge system capabilities is now complicated by the increasing integration of the Services' computing, intelligence, surveillance, reconnaissance and electronic warfare systems. There are further complications from the need to integrate into command support systems the data from administrative, personnel, logistics and resource output management systems. Such coupling of data and information is essential to allow commanders to make sound decisions

---

[24] With the introduction of Program Management and Budgeting in 1990, Defence reorganised its structure from five to eight 'programs' (functional groups). The Defence Reform Program (1997) replaced this with 14 groups (reduced to 12 groups in July 1999). On 23 June 2000 Defence announced changes to its corporate governance structure. The changes included the formation of five Owner Support Executives, five Output Executives and four Enabling Executives. (*Defence Report 1988–89*, p.ix; *Defence Annual Report 1997–1998*, pp.38–39; Department of Defence *Reform of Defence Headquarters Staff* DEFGRAM No.221/99 20 August 1999 p.2 and Audit Report No.13 1999–2000 *Management of Major Equipment Acquisition Projects—Department of Defence* October 1999 p.44

rapidly—consistent with the expected tempo of modern military operations.

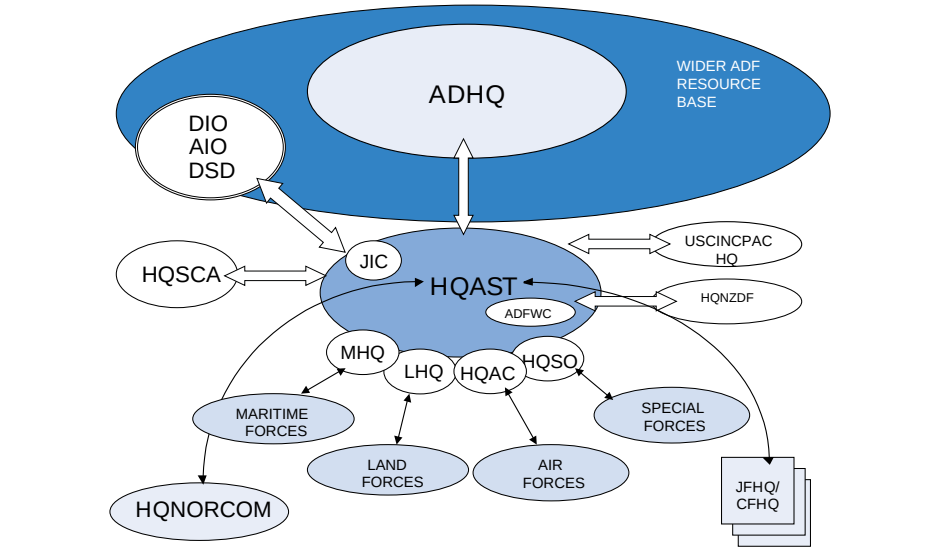
3.5 Increased integration increases the need for some form of centralised management that has the managerial flexibility to cope with wide-spread elements of the system as well as an ability to cope with changing technological environments. As cited in paragraph 2.9, Defence considers C[4]ISREW to be a 'system of systems' that *should be a virtual capability, delivering systems that provide superior situation awareness for commanders to exploit the Knowledge Edge.* This means that the knowledge system should be considered to be a 'virtual' output embodied in all Defence Outputs.

3.6 Command systems are critical to delivering Defence outputs and outcomes. Knowledge Staff advised the ANAO that all Output Managers need to be consulted on issues regarding command system priorities to ensure that the needs of joint and single Service operations are addressed. The three Service Chiefs contributed formally to capability development through the former Defence Capability Sub-Committee (DCSC), of which the Deputy Service Chiefs were members, and through the former the Defence Capability Committee (DCC), of which the Service Chiefs were members. Under the arrangements announced on 23 June 2000, the Output Managers remain members of the Chief of Staff Committee (COSC) and are members of a new Defence Committee.

3.7 This need for wide consultation means that whole-of-life, whole-of-capability management of Defence's knowledge systems is far more complex than the management of single Service capabilities. This increases the risk of inadequate linkage between the command system top-down planning and command system output management. This risk is addressed by the formation of the Knowledge Staff and the principal knowledge edge governance boards, that is, the Defence Information Environment Board and Defence Intelligence Board.

3.8 Figure 3 provides an indication of the organisational interrelationships that underpin the knowledge edge.

Figure 3
The Australian Defence Force's C³I Structure



ADF = Australian Defence Force	HQAC = Headquarters Air Command	JFHQ = Joint Force Headquarters
ADHQ = Australian Defence Headquarters	HQAST = Headquarters Australian Theatre	JIC = Joint Intelligence Centre
AIO = Australian Imagery Organisation	HQNORCOM = Headquarters Northern Command	LHQ = Land Headquarters
CFHQ = Coalition Force Headquarters	HQNZDF = Headquarters New Zealand Defence Force	MHQ = Maritime Headquarters
DIO = Defence Intelligence Organisation	HQSCA = Headquarters Support Command Australia	USCINCPACHQ = US Commander-in-Chief Pacific Headquarters
DSD = Defence Signals Directorate	HQSO = Headquarters Special Operations	

Source: Department of Defence

The knowledge system at the Theatre and operations levels[25]

3.9 The ADF's knowledge system and its supporting administrative systems are the nerve system and corporate knowledge system that are to allow the ADF to function efficiently. Increasingly, nations' defence forces are being asked to apply force in precise ways to produce 'tailored effects' that minimise unintended 'collateral damage'. Precision also reduces the use of consumables of all kinds. This enables operations to proceed with minimum inventories of ammunition, rations, fuel, spare parts and equipment positioned in forward operating areas. All this can dramatically reduce the logistics support task.

3.10 However, precision places heavy demands on the knowledge edge, particularly on intelligence, surveillance and reconnaissance systems and the speedy application of the data and information that flow from those systems. Managing with minimal logistics support calls for superior management of flexible logistics information systems.

[25] The Australian Theatre comprises any and all areas of operations in which ADF forces are operationally involved.

3.11 Heavy demands are also placed on command, control and communication (C^3) systems. In terms of ADF joint operations, the line of command is normally from the Chief of the Defence Force (CDF) to the Commander Australian Theatre (COMAST). COMAST commands operations, unless otherwise directed by CDF, and is responsible for campaign planning.

3.12 COMAST may exercise command of assigned forces, either directly or through:

- one of the four component Commanders (Maritime, Land, Air and Special Forces);
- Commander Northern Command (COMNORCOM); or
- Commander Deployable Joint Force Headquarters (DJFHQ), or a designated Joint or Combined Force Headquarters (CFHQ).[26]

3.13 C^3I services need to be based on a cohesive and integrated command and control architecture to support situational awareness; collaborative planning; command and control; force integration; and operations management. The ADF's C^3I embraces ADHQ, Headquarters Australian Theatre (HQAST), Headquarters Support Command Australia (HQSCA), and the theatre intelligence system provided by the Australian Theatre Joint Intelligence Centre (ASTJIC), which is connected to the Defence Intelligence Organisation (DIO) and the Defence Signals Directorate (DSD). The C^3I system also needs to be capable of interfacing with the C^3I systems of allied forces—see Figure 3.

Knowledge system at the Services level

3.14 Australia's Strategic Policy recognises the need for effective exploitation of information technologies in the following terms:

> *…Australian forces will always be small relative to the large areas they need to cover and the demands we make of them. Information technology applied to the command, positioning, and targeting of our forces will enable us to use our forces to maximum effect, and get most value from each unit.*[27]

---

[26] Department of Defence, *Australian Theatre C3I Strategy*, April 1999, pp.8–10.

[27] Department of Defence, *Australia's Strategic Policy*, 1997, p.57.

3.15 Defence has deployed and embedded communications, information, surveillance, reconnaissance systems and electronic warfare systems extensively throughout its various Force Element Groups (FEGs) within the Services. Most of these systems are acquired and logistically supported by the Defence Materiel Organisation.

3.16 Most Defence computer hardware, including standard data communication systems, is acquired and supported by the Defence Information Systems Group (DISG). Secret and Top Secret systems are supported by the Joint Systems Support Agency (JSSA), which is an agency of DISG. Defence Signals Directorate (DSD) also provides and maintains several highly-classified networks on behalf of the wider intelligence community.

3.17 Defence has five command support systems in operation:

- a core command support system—the Joint Command Support System (JCSS);
- an Air Force Air Command Support System (ACSS);
- an Army Battlefield Command Support System (BCSS);
- a Special Operations Command Support System (SOCSS); and
- a Navy Maritime Command Support System (MCSS).

These systems operate at the Secret level of classification. They began largely as separate systems but, in recent years, considerable effort has been made to put them into a common growth path that will ensure increasing levels of interoperability, while retaining capabilities that meet the unique requirements of each of the three Services.

Command support systems

3.18 Command support systems provide data, such as logistics, readiness, operational and environmental data, for use in situational awareness, planning, decision-making and capability enhancement.

3.19 In the past, the ADF's command support systems, such as Army's ongoing $165 million Battlefield Command Support System (BCSS—formerly known as AUSTACCS) and Air Force's Air Command Support Systems (ACSS), were developed primarily for a single Service. Defence formed HQAST in 1995 and some projects took on a joint-Service form and title. Examples are the Joint Command Support System (JCSS), which now incorporates the ACSS as an integral phase and component, and the Joint Intelligence Support System (JISS).

Intelligence systems

3.20 Military intelligence capability is centred on Defence Sub-output 5.1 (Strategic Intelligence), which contains the three central intelligence organisations: DSD, DIO and AIO. The intelligence function is integrated into the command system mainly through the JISS and the Australian Theatre Joint Intelligence Centre (ASTJIC) in Sydney, Headquarters Northern Command (HQNORCOM) in Darwin and the ADF Intelligence Coordination Centre (ADFICC) in Canberra.

Surveillance, reconnaissance and electronic warfare systems—SREW

3.21 The surveillance, reconnaissance and electronic warfare system elements of C^4ISREW are dispersed among many outputs. For example, Sub-output 4.3 (capability for strategic surveillance) and Sub-output 4.1 (capability for air strike and reconnaissance) are the Chief of Air Force's responsibilities. Surveillance and reconnaissance data are accessible to commanders through numerous systems including the JISS, JCSS and DSTO's Technology Demonstrator Recognised Air Picture (TDRAP).

3.22 Defence's surveillance system is now being integrated with those of other Government agencies. Defence provides Coastwatch with maritime and air surveillance assets. In 1999–2000 Defence allocated to Coastwatch surveillance 250 RAAF P3–C Orion Maritime Patrol aircraft flying hours and 1800 RAN Fremantle Class Patrol Boat steaming hours.[28] As a result of decisions taken on the basis of the Prime Minister's Coastal Surveillance Task Force report, Defence and the Australian Custom Service's (ACS's) Coastwatch sub-program have established the National Surveillance Centre (NSC) at ACS headquarters in Canberra.[29] The NSC brings together data from national intelligence, Defence surveillance, Customs and other sources to help ensure Australia's surveillance response assets are carefully tasked and well informed.

3.23 Also, each of the three Services has specialised electronic warfare systems that relate to specific platforms and weapon systems, but often do not account for the increasingly joint nature of military operations. Defence has recognised this by initiating a force-level electronic-warfare project, known as Project Bunyip, as a first step to overcoming the segmentation and limited interoperability of current capabilities in this area.

---

[28] ANAO's Audit Report No.38 1999–2000 *Coastwatch Australian Customs Service* pp. 36, 65, 66–76, 77.

[29] C4ISREW Staff comments on ANAO Discussion paper, *Command System Projects in Defence*, 23 June 2000, p.19.

Administrative information systems

3.24 Integral to effective C[4]ISREW are the administrative information systems containing data on personnel (medical, training), logistics and preparedness. The administrative computing infrastructure supports the management of every aspect of Defence business, including supply, personnel and finance. Defence has tens of thousands of desktop computers in over 300 locations connected to networks.[30]

3.25 Defence uses numerous management information system infrastructures and corporate applications to support Defence outputs. Most of these systems are developed by individual business process owners, with DISG providing production support and much of the technical infrastructure. The principal systems are:

- Resource and Output Management Accounting Network (ROMAN);
- the Services' capability management systems, such as the information systems that support the Navy's capability management framework;[31]
- Standard Defence Supply System (SDSS); and
- Personnel Management Key Solution (PMKEYS).

Conclusion

3.26 This Chapter highlights the organisational complexity faced by the knowledge system managers. Defence's total knowledge system consists of a vast system of systems. It is necessarily decentralised across all outputs, but it demands centralised management to preserve integrity and maximise synergies. Defence's new approach to knowledge system management is to regard the knowledge system as a virtual output and to manage it accordingly. This seems to be a sound approach, since it provides the required focused responsibility, accountability and authority for formulating and adopting strategies and plans for knowledge system policy and capability development, as discussed in Chapter 2 (paragraphs 2.8–2.18).

---

[30] Address by Mr Patrick Hannan, Chief Information Officer—Defence, Head Defence Information Systems, Defence Watch Seminar, 12 August 1999. p.8.

[31] The Navy's Capability Management Framework is based on activity based management (ABM), which consists of four major components: a Performance Management Framework (PMF), a readiness measurement system (Management of Navy Integrated Assessment Report—MONICAR), and Navy Sustainability Predictive Modelling.

4. Difficulties in Managing Knowledge System Projects

This final chapter brings together the ANAO's assessment of key management difficulties faced by the Chief Knowledge Officer and concludes each section with a recommendation.

Future architecture of Defence Information Environment

4.1 The task of improving the synergies and coherency of Defence's knowledge systems will require the Knowledge Staff, with the backing of the Defence Information Environment Board, to examine all significant equipment and application projects, approved and planned, in terms of their contribution to, and dependence on, the DIE. The objective is to create the ability to move information readily to any areas within the DIE that might have a legitimate need for particular information and to apply the required information to a particular purpose.

4.2 A way of examining the projects is through the use of information architectures that facilitate a more disciplined approach to managing the structure of organisation components and their interrelationships, and with regard to the principles and guidelines governing their design and evolution over time. Like the UK MoD, US DoD and Canadian DND/CF, Defence has adopted this method (see paragraphs 2.10–2.18 and Appendix 3 paragraphs 8, 15, 16 and 19) and is developing the necessary core architectures to do so.

4.3 This work needs to have priority but has encountered difficulties caused by lack of coherence among Defence's underlying business processes. It is important to note that there is a close interaction between business process reform and information architecture development. This relationship is evolutionary and iterative and requires positive cooperation between the Chief Knowledge Officer, Chief Information Officer and the Chief Finance Officer.

4.4 The Defence corporate governance and accountability changes announced on 23 June 2000 allow for greater alignment of Defence business processes and therefore provide better opportunities for developing coherent architectures for Defence business systems.

Recommendation No.1

4.5 The ANAO *recommends* that, to assist the formulation and adoption of strategies and plans that promote coherence among information systems, Defence give priority to articulating an architecture (or architectures) for the future Defence Information Environment.

Defence response

4.6 Agree.

Chief Knowledge Officer scrutiny of military projects

4.7 On behalf of the Chief Knowledge Officer, Knowledge Staff are establishing the processes needed for effective program management of the projects that they sponsor. There were 50 such projects at the time of audit. Subject to some caveats discussed later, processes to achieve good coherence between these projects are now being put in place. Knowledge Staff are confident of achieving improved coherency between these projects. The importance of that achievement should not be underestimated, and if successful, it should result in much improved knowledge system capability.

4.8 The situation is much less clear for the many other projects, estimated to cost some $4 billion, that will contribute to, or depend on, the Defence Information Environment. As mentioned in Chapter 1, these include the proposed $2.2 billion Airborne Early Warning and Control Project, which is being managed as an air defence system acquisition.[32] Also included are ADF intelligence and electronic warfare systems and other systems acquired for national intelligence purposes. The Defence Intelligence Board is responsible for coordinating design, acquisition and through-life support of a number of relatively small national intelligence projects.

4.9 With regard to the projects that the Chief Knowledge Officer does not sponsor, the former C[4]ISREW Staff informed the ANAO as follows:

> *C4ISREW Staff have less confidence about the ability of the ADF's tactical fighting platforms / units and many of the surveillance systems to adequately exchange the information needed to support their*

[32] Department of Defence, *The Commonwealth's AEW&C Requirement*, 21 July 1999, available: http://www.dao.defence.gov.au/aad/ASS/air5077/AEW&CRequirement/require.htm

operations. Although the project approval mechanism is well defined, there are few underlying processes that support the system designers and acquirers to ensure their actions are consistent with the architecture of the broader DIE or a process to propose changes to it.[33]

4.10 This advice indicates the existence of program management weaknesses in the past. However, it is not clear that processes are now sufficiently robust to allow the Chief Knowledge Officer to scrutinise these projects adequately and, where appropriate, to challenge a perceived lack of coherency between the project and the Defence Information Environment. The coverage of must be extensive; from radio spectrum management[34] at one end of Defence's information continuum, to the selection of computer applications software at the other.

4.11 Improving coherence between a project and the Defence information environment may prove costly. Even testing for coherence may be costly, since 'paper' evaluations and simulations are not sufficient for identifying all inadequacies in coherency between systems. Test ranges and exercises need to be realistic but can be expensive.

4.12 However, knowledge system coherence and integration have substantial benefits from Defence's military and business process perspectives, and hence should be pursued. It would seem inappropriate for the costs of improving coherence between projects and the Defence information environment to be met by the Chief Knowledge Officer. The Chief Knowledge Officer, in this respect, is simply the guardian of the environment. Acquisition projects should meet the necessary environmental standards before they are approved and again before they are admitted into service.

4.13 Conversely, it would seem inappropriate for Knowledge Staff to spell out the proposed future characteristics of the Defence information environment and leave it to project managers to decide how much coherency would be achieved between particular projects and the DIE. This would be inconsistent with the program management charter given to, and the expectations of, the Chief Knowledge Officer and the Knowledge Staff.

---

[33] C4ISREW Staff, *Comment on Audit Discussion Paper 3 Coherency in the DIE*, 16 June 2000, p.3.

[34] A recent internal Defence report indicates that Defence is experiencing radio spectrum management problems—*Defence Spectrum Planning Review—A Report Prepared for the Director General C3I Development*, 8 February 2000 discussion draft.

4.14 However, improved coherency between information systems should not be an end in itself. The objective must always be to enhance the ability of front-line personnel to apply military force with precision in a wide range of possible circumstances.[35] This 'ability' must be subject to central military command and control. Knowledge system capability cost and benefit trade-offs must be made in the context of Defence as an integrated military organisation.

4.15 Defence's corporate governance changes, announced on 23 June 2000, include the formation of Owner Support Executives, who are to support the governance role and are to focus on Government and its role as owner of the enterprise.[36] The Chief Knowledge Officer, as part of the Owner Support Executive, and with the program management responsibilities detailed in paragraph 2.8, will need the accountability, responsibility and authority of a Program Manager. Since knowledge systems are pervasive throughout Defence, it is difficult to delineate a knowledge systems program. However, it is clear that knowledge system projects comprise a program within the organisation.[37] This is a powerful concept and indicates the authority appropriate to the Chief Knowledge Officer as the manager of a key program in Defence.

Recommendation No.2

4.16 The ANAO *recommends* that Defence develop more-disciplined program management processes by which the Chief Knowledge Officer can scrutinise military projects not sponsored by him and, when appropriate, require improvements in the coherency between those projects and the Defence Information Environment.

Defence response

4.17 Agree.

---

[35] Such circumstances may range from peacekeeping operations *to future military challenges that may require quite different forces*. See Paul Dibb 'A Trivial Strategic Age?' in *Quadrant* July—August 2000 pp.11–17; particularly his comments regarding the RMA, p.14.

[36] Op cit *Defence Governance and Accountability*, p.4.

[37] There is some support for this view from the UK Central Computer and Telecommunications Agency, whose work is relevant to Defence's reforms in this area. The Agency defines program management as:

> *…a structured framework for defining and implementing change in an organisation. The framework covers organisation, processes, outputs and ways of thinking that focus on delivering new capabilities and realising the benefits of these capabilities* (Central Computer and Telecommunications Agency, *Managing Successful Programs* 1999 p.9).

Chief Knowledge Officer scrutiny of administrative systems

4.18 Administrative systems assist in financial, personnel, logistics and information management functions. Defence uses about 150 separate logistics systems and many personnel and administrative information management systems. This is a result of business processes that allowed managers to acquire information systems to satisfy their individual functional requirements. The degree of commonality and ability to exchange information between these systems is limited.

4.19 From an information coherence perspective, Defence's business systems are the area of greatest concern to the Chief Knowledge Officer's staff. Defence's recent deployment to East Timor brought these issues to notice. The Knowledge Staff advised the ANAO that:

> *Operations in East Timor reinforced the need for commanders to have access to the information held in our business applications. These commanders had difficulty tracking personnel movements, producing deployment planning sheets and tracking logistics.*[38]

4.20 This advice indicates significant work remains to be done to overcome Defence's information systems deficiencies that were reported to the Defence Program Management Committee in 1996 as follows:

> [the systems in the main]…*have been developed to meet specific needs with little regard for wider application of the information they collect and maintain. As a result, even where the systems were physically compatible, substantial work would be required before the information could usefully be shared.*[39]

4.21 To improve that situation, Defence formed the Defence Information Management Board (DIMB). Chaired by the then Defence Chief Information Officer, DIMB brought together eight functional group Chief Information Officers (CIOs). All the CIO positions were part-time.[40] However, in 1997 the Defence Efficiency Review Secretariat reported

---

[38] C4ISREW Staff, *Comment on Audit Discussion Paper 3 Coherency in the DIE*, 16 June 2000, p.1. See also updated advice in DHQ 99/24424 C3ID, 18 July 2000.

[39] Defence Program Management Committee, Agendum No. 08/1996 (Revised), *Information Management Arrangements in Defence*, 19 June 1996, p.3.

[40] Department of Defence, *Future Directions for the Management of Australia's Defence, Addendum to the Report of the Defence Efficiency Review—Secretariat Papers*, March 1997, p.112. See also *Defence Annual Report 1996–1997*, p.178.

that the DIMB relied on consensus to find solutions to information management problems and therefore *lacked the ability to enforce effectively the development of a corporate direction.* The Defence Efficiency Review reported that:

> *A Defence Information Organisation is needed for drawing together policy and planning; operations support for in-service systems; development of new capabilities; and management of the communications infrastructure. The medium term goal for Defence should be a single Information Management Organisation which combines operational and administrative systems. The scale of current deficiencies and challenges concerning Defence management of information identified by the Review would, we believe, preclude this approach in the short term. Although we consider that operational and administrative systems should be treated together, initial division of these functions will enable a more effective redress process to be initiated by Defence.*[41]

4.22 In 1998 ADHQ developed the Defence Information Environment (DIE) concept and replaced the DIMB with the Defence Information Environment Board (DIEB), chaired initially by Deputy Secretary Corporate, then VCDF from July 1999. An August 1999 reorganisation moved the Chief Information Officer (CIO) responsibilities from the ADHQ's DepSec Corporate to the Head Defence Information Systems Group (HDISG).

4.23 The division remains between:

- knowledge systems sponsored centrally by VCDF or the Chief Knowledge Officer; and
- administrative information systems (administrative systems) sponsored by individual business process owners.

4.24 The East Timor experience confirms the need for the Chief Knowledge Officer to scrutinise Defence's business and other administrative systems and assess their coherency with the Defence Information Environment.

---

[41] Department of Defence, *Future Directions for the Management of Australia's Defence, Report of the Defence Efficiency Review*—March 1997, p.53.

Recommendation No.3

4.25 The ANAO *recommends* that Defence develop formal transparent processes to allow the Chief Knowledge Officer to scrutinise the future development of Defence's administrative systems and assess their coherency with the Defence Information Environment.

Defence response

4.26 Agree.

Coherency between knowledge systems during acquisition

Chief Knowledge Officer as customer

4.27 Changes to the high-level structure of Defence announced on 23 June 2000 included the formation of the Defence Materiel Organisation (DMO) as an Enabling Executive.[42] The DMO's role is to provide services to the Output Executives and the Owner Support Executives.

4.28 This clarification in roles will help to overcome weaknesses that were apparent in the previous arrangement. Previously, when new projects sponsored by the then Head C[4]ISREW passed to Defence Acquisition Organisation, the status of the Head C[4]ISREW as customer was unclear. He was the sponsor of the requirement, but that is less than being a customer. The new arrangement will help to make clear that, during acquisition, the Chief Knowledge Officer is the customer for projects that he sponsors. When acquisition is complete, responsibility for management of the products accepted into service will pass to the Output Executives. It will also help to reduce the hiatus associated with moving a project from proposal to acquisition and on into service.

4.29 This arrangement will parallel practices recently introduced in the UK Ministry of Defence—see Appendix 3. Nevertheless, in line with the changes in Defence, the Chief Knowledge Officer's role as customer needs to be clarified.

Proposal for an integration authority

4.30 As indicated below, the recent changes in the UK include another innovation that Defence could consider adopting.

---

[42] DMO comprises the former Defence Acquisition Organisation and Support Command Australia

4.31 Numerous Defence acquisitions have an impact on the Defence information environment but are not sponsored by the Chief Knowledge Officer. They fall into two categories. The first category, mentioned in paragraph 1.10, are major projects categorised as system or platform projects, such as the Airborne Early Warning and Control Project. The second category are minor capital projects that cost less than $20 million or do not have Defence policy or joint-Service implications. These projects are initiated by many different parts of Defence, especially the three Services. The Owner Support Executives do not have detailed visibility of these projects. Proponents of these minor capital projects assert that expenditure on them is handled more efficiently than expenditure on major projects and that this arrangement should not be disturbed.

4.32 During the acquisition of projects of both categories, many technical decisions are taken that can and do seriously affect the DIE's integrity and coherence. Cutting corners on DIE coherency is a temptation to project managers under time and cost pressures and must be avoided through adequate managerial control.

4.33 The UK MoD recently addressed the need for formal management of integration issues during acquisition by establishing an Integration Authority in its Defence Procurement Agency (DPA). The Integration Authority's purpose is to maintain technical visibility of all relevant projects under procurement and to bring to attention any developments that could adversely affect information coherency (see Appendix 6).

4.34 The ANAO sees merit in Defence adopting a similar arrangement here, and notes that there would need to be a close working relationship between an Integration Authority and the Chief Knowledge Officer. Knowledge Staff advised the ANAO that a proposal for such an arrangement here would need careful consideration and that Defence would need to:

- consider the appropriate degree of central supervision of the acquisition process to ensure DIE coherency without delaying the acquisition process and complicating the task for managers of projects that do not have a substantial C^4ISREW component;
- assess the level of resources needed and available for different levels of central control; and
- decide which organisation is to be responsible for ensuring information coherency in the acquisition phase.

Recommendation No.4

4.35 The ANAO *recommends* that Defence:

a) clarify the Chief Knowledge Officer's role as the customer for acquisition projects that he sponsors; and

b) consider the costs and benefits of establishing an Integration Authority, along the lines of that established in the UK Defence Procurement Agency.

Defence response

4.36 Agree.

Standardised Project Management Method

4.37 An effective and consistently applied standard project management method provides an important foundation for good program management by establishing, for each project in the program's portfolio of projects, a set of concepts and project management processes that are the minimum requirements of a properly run and managed project. Defence is now establishing the major organisational structures and business processes needed to interface with program management. The business processes of most significance are Defence's Standard Project Management Method (SPMM) based on the UK Central Computer and Telecommunications Agency's *PRINCE 2* and the Agency's approach to program management which is now being considered by Knowledge Staff and the Defence Materiel Organisation (DMO).[43]

4.38 The Defence acquisition reform program presently being implemented seeks to have the SPMM applied to all 200 or so major acquisition projects by July 2000.[44] However, progress indicates that not all acquisition projects will be converted to SPMM until 2001. Moreover, there appear to be problems in achieving effective application of the SPMM. As at April 2000, for example, there were 64 acquisition projects subject to the SPMM but only two of these were assessed as controlling their projects well using the SPMM.

---

[43] Central Computer and Telecommunications Agency *Managing Successful Projects with PRINCE 2* 1999. See also Central Computer and Telecommunications Agency *Managing Successful Programs* 1999.

[44] Audit Report No.13 1999–2000 *Management of Major Equipment Acquisition Projects—Department of Defence*, October 1999, pp.56–69. ADHQ, *Defence Whole of Capability, Whole of Life Implementation Plan*, May 2000.

4.39 Training in *PRINCE* is regarded as essential for all staff in VCDF's Owner Support Executive engaged in capability development. Knowledge Staff advised the ANAO that VCDF has made a strong commitment to the formation of Integrated Project Teams (IPTs) that are part of ADHQ's SPMM. DMO advised the ANAO that:

- the Head of the Defence Information Systems Group decided recently to adopt *PRINCE* as the way in which his staff will manage a myriad of business systems projects; and
- Support Command Australia, now part of DMO, recently put its management of minor projects under scrutiny with a view to maximising commonality between the way each of the three Services manages its element of the minors program. All three essentially follow *PRINCE* principles.

4.40 The DMO is providing training in its SPMM for Defence personnel engaged in major acquisition projects. Statistics of the extent of this training are contained in Appendix 7. The statistics indicate that more than half of Defence's project management personnel are still to be trained in the SPMM. Late in the audit a private firm completed a Training Needs Analysis covering the efficiency and effectiveness of DMO's SPMM and Integrated Acquisition Teams (IATs) that are a part of the SPMM. The analysis identified areas of concern and made 12 recommendations regarding future training needs, training administration, SPMM and IAT implementation, and *PRINCE 2* accreditation.[45]

4.41 The ANAO endorses the moves to apply formal SPMM in Defence, and the periodic use of the *PRINCE 2* Healthcheck in all Defence projects that have been converted to SPMM.[46] However, further action appears desirable to not only ensure that SPMM in Defence is not applied in too many variations, but also to remove any confusion about the role of SPMM and any associated Project Boards, Integrated Product Teams, Integrated Acquisition Teams and Integrated Project Teams.

---

[45] Elizabeth Morse Consulting *Report to Defence Acquisition Organisation on Training Needs Analysis* Final Report, 27 June 2000.

[46] Central Computer and Telecommunications Agency *Managing Successful Projects with PRINCE 2* 1999 pp.331–336.

Recommendation No.5

4.42 The ANAO *recommends* that Defence carefully monitor its adoption of the Standard Project Management Method (SPMM) to ensure that core and essential elements have a high degree of consistency across Defence.

Defence response

4.43 Agree.

Progress in adopting new acquisition methods

4.44 A report by the Defence Science and Technology Organisation (DSTO) identified problems in developing C^3I capability. DSTO believes that the effectiveness of modern C^3I systems depends to a large extent on the latest technologies. Any delays in incorporating those technologies necessarily compromise the effectiveness of the systems or capability. Such delays, combined with the long time-scales inherent in contemporary acquisition practices, mean that systems are often fielded with obsolete equipment; require expensive upgrades shortly after delivery; and are delivered late because time was spent implementing requirements that changed during the course of the project.[47]

4.45 A DSTO survey in 1999 found evidence of excessive time being taken by Defence to acquire systems. Requests for tender and source selection processes were frequently cited as activities that consume excessive time. Invitations to register interest can affect industry's interactions with each other, and with Defence. This can also result in delays and additional workload for acquisition staff.[48]

Evolutionary acquisition method

4.46 DSTO believes that the Evolutionary Acquisition (EA)[49] project management technique can deliver functionality sooner than other acquisition methods, and that it should be adopted for a range of projects, from software intensive projects to projects with less software complexity but subject to high rate of technological change. However, DSTO has found that, even though EA has become an approved acquisition strategy in Defence, there is a widespread view in Defence that EA guidance is either lacking or poorly developed and that EA's full potential is not being realised.[50] DSTO recommended that appropriate action be taken

---

47 Department of Defence, Defence Science and Technology Organisation *Problems in the Iterative Development of C^3I Capability* DSTO–RR–0167, November 1999, pp.12–13.

48 Ibid.

49 See Glossary.

50 Department of Defence, DSTO–RR–0167 loc. cit. pp.14–17.

to address, among other things, the development of EA guidance and that the method be applied to a wider spectrum of projects.

4.47 Acquisition staff advised the ANAO in February 2000 that Defence has limited experience in EA and is still evolving the means for determining the transitions that distinguish evolutionary acquisition costs from in-service upgrades. For example, during the audit the former DAO advised that it had difficulty with the JISS project's transition point between evolutionary acquisition and in-service support.[51] That point needs to be better defined in order that in-service upgrade costs may be distinguished from the project's evolutionary acquisition costs. DAO advised that this need frequently occurs in information systems.

Recommendation No.6

4.48 The ANAO *recommends* that Defence assess the priority to be given to exploiting the advantages of Evolutionary Acquisition methods, particularly for projects with a significant impact on the Defence Information Environment and take the requisite action.

Defence response

4.49 Agree.

Qualified and experienced DIE personnel

4.50 The military and civilian workforce that supports the Defence Information Environment (DIE) is spread across a wide range of projects and endeavours. In practice, it has been necessary to address shortages of skills in one area by denying essential skills to another. Defence's information environment is vulnerable to shortages in staff with the appropriate skills and experience.

4.51 Statistics provided by Defence indicate that the Services encounter difficulties in recruiting and retaining the highly-skilled personnel needed to support the DIE, whether in the single Service or in the joint domains. This also applies to Defence's civilian employees with similar skills. The employment market for communications and computing specialists, and knowledge workers such as intelligence specialists, policy officers and project staff, is such that many Defence employees are attracted to jobs in the wider community.

[51] DAO e-mail, *ANAO Audit of Command System Projects in Defence*, 23 February 2000, p.1.

4.52 The ANAO recognises Defence's difficulties in this area but considers that, in view of the substantial risks to knowledge projects and the importance of maintaining the DIE at a high level of capability, there is a need for more formal and holistic planning and management of the DIE workforce.

Recommendation No.7

4.53 The ANAO *recommends* that Defence undertake formal workforce planning and management assessments of the Defence Information Environment workforce to ensure that training, postings, career prospects and professional development are carefully planned and that a holistic view, at least in a strategic sense, is taken in relation to these matters.

Defence response

4.54 Agree, with qualification. The management of Defence's Information Environment workforce is a complex issue. Workforce management arrangements for Defence Information Environment specialists cross the boundaries of responsibilities of the three Services and Public Service arrangements. The degree to which centralised control is required is unclear.

Management issues concerning the Defence Information Environment workforce have parallels with a Defence initiative to develop a joint logistic eduction and training policy. Defence will adopt a similar approach to the information workforce. The Chief Knowledge Officer, with other stakeholders, will initiate a study of these issues to better determine the requirement for centralised workforce planning of information specialists. This study will improve the understanding of the implications of the current situation and identify strategies for improvement.

Conclusion

4.55 Management of knowledge system projects in Defence is a complex and demanding task that should not be underestimated. This chapter necessarily focused on some key difficulties experienced in managing the knowledge system projects and the work that needs to be done in the future. Much of the work that remains to be done has not been achieved in Defence before. It is ground-breaking work that the Chief Knowledge Officer and his staff in the main have responsibility for.

4.56 Corporate governance and accountability changes announced in June 2000, and to be finalised in October 2000, may provide the Chief Knowledge Officer with authority and accountability commensurate with

his program management responsibility. However, some tasks critical to knowledge system development, such as the even application of a standardised project management method and improvement in acquisition methods, are in part the responsibility of others such as Defence Materiel Organisation and the Defence Information Systems Group.

4.57 The Chief Knowledge Officer and his staff have made a creditable start on developing some foundation management concepts and processes necessary to monitor and control knowledge system program risks. The goal of building a knowledge system based on a coherent architectural framework is necessarily long-term and challenging, given the rapid advances in technology, wide-ranging tasks that the ADF may be called on to perform and Defence's evolving organisational relationships and business processes. The Chief Knowledge Officer and his staff have much to do to bring the Defence information environment under adequate managerial control. Many knowledge system elements now in service were selected on the basis of individual functionality and not on the basis of their architectural compliance with the broader system of systems.

4.58 The program management and architectural goals are worthwhile due to the many substantial benefits that knowledge system coherence and integration will provide from Defence's military and business process perspectives. Critical success factors relate to the degree of program management discipline that can be applied to knowledge edge development and maintenance. The most substantial risks to knowledge system projects may be those associated with development and retention of skilled individuals needed in all parts of the Defence information environment.

Canberra A.C.T.
15 September 2000

P. J. Barrett
Auditor-General

Appendices

Appendix 1

Knowledge System Projects Sponsored by Chief Knowledge Officer

1. Table 1 lists the approved major capital equipment (White Book) projects sponsored by the Chief Knowledge Officer. These projects will cost an estimated $4.5 billion. There will be other costs such as:

- the operating costs of extant information systems at the strategic, operational and tactical levels;
- the costs of new information systems purchased outside the Capital Equipment Program, by organisations such as DISG and Support Command; and
- personnel and training costs.

2. The list does not include some large approved major projects such as the Airborne Early Warning and Control project (AIR 5077) and Rotary Wing for Land Force project (AIR 87) that will undoubtedly influence the Defence Information Environment (DIE). However, it is not the practice to classify these other projects, which are sponsored elsewhere in Defence, as 'DIE projects'. Consequently, the estimated total of $4.5 billion for projects listed in Table 1 is only part of the estimated total of $8.5 billion for all 'knowledge system' projects (estimated in Defence's April 1999 audit of current and planned knowledge system projects).

Table 1

Approved Knowledge System Projects sponsored by Chief Knowledge Officer, May 2000

Project No	*Project Name*
DEF 20 PH 1	ADVANCED COMPUTER TECHNIQUES
DEF 222 PH 1	CLASSIFIED PROJECT
DEF 333 PH 1	CLASSIFIED PROJECT
DEF 444 PH 1	CLASSIFIED PROJECT
DEF 7013 PH 1	ADF DISTRIBUTED INTELLIGENCE SYSTEM
DEF 7013 PH 2	JISS
DEF 7013 PH 3A	JISS
DEF 7013 PH 3B	JISS
DEF 777	CLASSIFIED PROJECT
DEF 888 PH 4	CLASSIFIED PROJECT
JP 2008 PH 2	MILSATCOM—DMCN ACQUISITION
JP 2008 PH 3C	MILSATCOM—THEATRE BROADCAST SYSTEM
JP 2008 PH 3D	MILSATCOM—MILITARY SATELLITE PAYLOAD
JP 2025 PH 2B	JINDALEE RADAR NETWORK

continued next page

Project No	*Project Name*
JP 2025 PH 3/4	JINDALEE RADAR NETWORK
JP 2030 PH 2	ADF JCSE
JP 2030 PH 3	ADF JCSE
JP 2030 PH 4A	ADF JCSE
JP 2030 PH 5A	ADF JCSS
JP 2030 PH 5B	ACSS
JP 2030 PH 7	JCSS/ACSS
JP 2034	MINIMUM ESSENTIAL EMERGENCY NETWORK
JP 2036 PH 1	NARROWBAND SECURE VOICE EQUIPMENT
JP 2039 PH 1	EASYCOM
JP 2042 PH 1A	BLUEFIN
JP 2043 PH 1	HF MODERNISATION
JP 2043 PH 3A	HF MODERNISATION
JP 2046 PH 1	1 RSU FREQUENCY MANAGEMENT SYSTEM UPGRADE
JP 2047 PH 0	DEFNET
JP 2049 PH 1	MULTI-LEVEL INFORMATION SECURITY
JP 2049 PH 2	MULTI-LEVEL INFORMATION SECURITY
JP 2054 PH 1	DEFENCE MESSAGING & DIRECTORY ENVIRONMENT
JP 2056 PH 1	DJFHQ
JP 2058 PH 1	HQNORCOM UPGRADE
JP 2061 PH 1	C31 TECHNOLOGY DEMONSTRATOR (EXC3ITE)
JP 2064 PH 1	MERMAID
JP 42 PH 2A	DIGITAL TOPOGRAPHICAL SUPPORT
JP 65 PH 4	FIELD DIGITAL TRUNK COMMUNICATIONS
JP 65 PH 6	PARAKEET
JP 65 PH 7A	PARAKEET
JP 8001 PH 1	COLLOCATED JOINT HEADQUARTERS
JP 8001 PH 1B	HEADQUARTERS AUSTRALIAN THEATRE
LAND 122 PH 2	WAGTAIL TACTICAL RADIOS
LAND 42 PH 1	PARARE DIGITAL TOPOGRAPHICAL SUPPORT
LAND 49 PH 3	SINGLE CHANNEL RADIO SYSTEM (RAVEN)
LAND 49 PH 4	SINGLE CHANNEL RADIO SYSTEM (RAVEN)
LAND 50 PH 1	ELECTRONIC WARFARE SYSTEM—ESM SUB SYSTEM
LAND 50 PH 4	ELECTRONIC WARFARE SYSTEM—ESM SUB SYSTEM
LAND 75 PH 3.2	BCSS
SEA 1420 PH 1	SATCOM FOR COLLINS CLASS SUBMARINE

Note: the approved cost of these projects is not disclosed publicly at present.

Appendix 2

Defence Information Environment Board

1. The Defence Information Environment Board (DIEB) comprises the command system stakeholders shown in Table 2. Its function is to oversee the investments in the DIE and to:

- endorse continuing changes to the DIE Strategic Plan;
- endorse significant DIE related project proposals prior to their consideration by the Defence Capability Committee (DCC)—now known as the Defence Capability and Investment Committee (DCIC);
- consider the relative priorities of DIE activities and investments;
- endorse high-level Information Management policy; and
- report to the Defence Executive on the condition of the DIE.

2. The DIEB meets quarterly. It includes key DIE stakeholders categorised as Output Executives (users of the DIE); the Enabling Executives (those accountable for delivering DIE products); and the Owners Support Executive (ultimately accountable for overall DIE capability development).[52]

Table 2

Defence Information Environment Board—Program Management Relationships

Owners Support Executives:
Vice Chief of the Defence Force (Chairman)
Chief Knowledge Officer (Deputy Chairman)
Head Capability Systems

Output Executives (users):	**Enabling Executives (suppliers):**
Deputy Chief of Navy	Head Defence Information Systems Group
Deputy Chief of Army	Head Systems Acquisition (Electronic Systems) DMO
Deputy Chief of Air Force	Director Electronic Systems Research Laboratory DSTO
Commander Australian Theatre	Commander Support Australia DMO
Director Defence Intelligence Organisation	Head Defence Corporate Support
Director Defence Signals Directorate	**Permanent Invited Adviser:** Assistant Secretary Security

Source: Prepared by the ANAO from Defence records

[52] The DIEB replaced the Defence Information Management Board (DIMB), which was formed in 1997. The DIMB brought together each Group's Chief Information Officers (CIOs) to consider portfolio information technology issues.

Appendix 3

UK, US and Canadian Experience

Introduction

1. The audit team, accompanied by a Defence command system development specialist, visited selected defence organisations in the UK, US and Canada. These organisations have been dealing with knowledge edge related equipment acquisition problems for longer and on a larger scale than the ADF, and, despite continuing difficulties, have developed some workable solutions. The aim of the visit was to learn from this experience.

2. The three countries' defence organisations indicated that, with continued rapid technological change, they find it difficult to achieve adequate coherency between information systems needed by joint force[53] and coalition force[54] operations.

3. This appendix summarises the main developments and views expressed to the ANAO.

UK Ministry of Defence experience with Information System Program Management

Ministry of Defence's Smart Procurement Initiative[55]

4. The *Strategic Defence Review* (SDR) of 1998, which reported on the future direction of British Defence policy, included a Smart Procurement Initiative (SPI) to ensure that future equipment procurement was 'faster, cheaper and better'. The SDR, prepared with assistance from the consultancy firm McKinsey & Company, identified clearly the need to move from a *functionally* based management and reporting structure to a *project* based organisation based on Integrated Project Teams (IPTs). The IPTs bring together all stakeholders and involve Industry (except during competition phases) under a team leader, normally selected from the Defence Procurement Agency (DPA). The IPTs are authorised to make

---

[53] A joint force comprises more than one of the three Services (Navy, Army and Air Force) of a nation's defence force.

[54] A coalition force comprises the defence forces of two or more nations.

[55] Ministry of Defence (UK) 1998 *Strategic Defence Review: White Paper* [online] available: http://www.mod.uk/policy/sdr/index.htm [21 June 1999]; Ministry of Defence (UK) 1999 *Smart Procurement Initiative: IPT Pilot Guide Edition 4* [online] available: http://www.mod.uk/policy/spi/iptguide /iptguide.htm [17 June 1999]; and Ministry of Defence (UK) 1999 *Smart Procurement Initiative: The MOD Acquisition Handbook* [online] available: http://www.mod.uk/policy/spi/handbook/front.htm [17 June 1999].

trade-offs between performance, cost and time within boundaries set by the approving authority. Functional links to policy-setting authorities outside the IPT remain, and members draw advice from those authorities.

Internal customer-supplier relationships

5. One of the key themes identified in the SDR analysis of Ministry of Defence (MoD) procurement was the need for clearer internal customer-supplier relationships. The creation of a single, central defence customer, the Capability Manager, in the Systems Area of MoD headquarters, and the clear definition of the relationship between this Central Customer and the IPTs, were seen as critical to achieving the full potential of the Smart Procurement Initiative. There is also a Second Customer, the appropriate Service Commander-in-Chief, who takes over the customer lead from the Central Customer when new equipment enters service.

6. The relationship between the Central Customer, and the supplier (the relevant IPT) is now formalised in Customer Supplier Agreements specific to each project and to each phase of the project. This gives the Customer more control throughout the procurement life-cycle. It also provides the supplier (the IPT) with a clear and unambiguous framework in which to operate and, within that, the flexibility it requires to meet agreed project deliverables.

7. The Central Customer, as represented by the Capability Manager, is solely responsible for tasking and reviewing the IPT's work. The Capability Manager looks across a broad range of capabilities and develops specific equipment concepts to meet capability gaps, guided by the Departmental Strategic Plan and the Equipment Plan. The MoD forms a Capability Working Group to support the Capability Manager as the need for a specific type of equipment becomes clear.

8. The Capability Manager for Information Superiority (CMIS) is tasked with selecting specific equipment concepts to meet information superiority capability gaps. The CMIS team use architectures that reduce complexity, increase flexibility and improve co-operation between people, processes and technology. The CMIS organisation uses two architectures: a business architecture that includes military operations, and an information and communication technology services architecture. According to the CMIS:

> *The pace of business change and technology advance is now so rapid that any attempt to produce, endorse or implement any form of strategy is considered questionable, unless that strategy concentrates only on these aspects that are enduring and which transcend such changes. A*

properly formulated architecture provides the means to capture these enduring aspects whilst providing a structured framework within which the more rapidly changing elements can be evolved and updated as a coherent whole.[56]

9. Capability Managers determine expenditure plans and set individual IPT budgets for operating and equipment costs. Once set, individual IPT budgets become constituent parts of the annual budgets of the DPA. The Capability Manager makes any necessary adjustments to planned expenditure on IPT projects between planning rounds and agrees to any changes to project progress and deliverables required to maintain in-year expenditure within the budgeted levels.

10. IPT Leaders manage resources within the annual budget set for their projects to deliver the agreed project outputs. They are directly accountable to the Capability Managers for delivering agreed targets and milestones. IPT Leaders are also accountable to DPA management for keeping expenditure within allocated resources while meeting agreed outputs and ensuring value for money, propriety and accurate accounting.

11. The relevant Capability Manager accepts the equipment into service when it meets agreed acceptance and verification criteria. When new equipment enters service, the Second Customer (the appropriate Service Commander-in-Chief) takes over the customer lead and agrees with the IPT on the level of ongoing equipment support, including availability and sustainability, to be provided.

12. The ANAO audit team had discussions with the CMIS and his Directors for Equipment Capability in the MoD's Central Customer organisation, and with several senior executives in the Defence Procurement Agency. The CMIS has a role similar to that of Defence's Chief Knowledge Officer.

13. Although the arrangements are new, MoD's and DPA's optimism about them appears to be justified by the Central Customer, IPT and Second Customer initiatives.

---

[56] ' Architecture' is used in its normal English sense, that is to describe 'a special method or style of structure and ornamentation' Oxford English Dictionary, or 'a unifying or coherent form or structure' Websters Dictionary. UK Ministry of Defence, Information Superiority Capability Manager, *Delivering Information Superiority—Architectures for Information Coherence in support of the Modern Battlespace and Information Age Government,* issue 1, 17 March 2000, pp. 5 and 8.

US Department of Defense experience in C4ISR Management

14. The US Department of Defense (DoD) and each of the three Services are supported by many C4ISR systems and platforms. These are designed to very specific requirements and are not highly interoperable in terms of presenting a common operating picture across all Services that allows commanders to achieve shared situational awareness.[57] Achieving interoperability between and among Service command and control systems is often difficult, and some Service communications systems must be put together on a case by case basis. This situation arises partly from the US law (United States Code Annotated Title 10, Armed Forces) which establishes each Service independently of the other two. Each year, Congress authorises funds to each Service to raise, train and equip its forces.

15. To promote C4ISR interoperability, the DoD has developed an architectural framework comprising a Joint Operational Architecture (JOA) which is the responsibility of Joint Chiefs of Staff, and a Joint Systems Architecture (JSA) and a Joint Technical Architecture (JTA) which are the responsibility of the Assistant Secretary for Defence—Command Control Communications and Intelligence (ASD- C3I). The operational and systems architectures are being developed concurrently. The architectures are reported to be widely understood and reasonably well accepted by the Services. Their development and evolution are being coordinated by the Architecture Coordination Council (ACC).[58]

16. The present goal of the Joint Technical Architecture is to facilitate C4ISR interoperability, covering the continuum spanning communication systems to computer applications, through an agreed set of technical standards. However, the number of technical standards is increasing with advances in Internet standards, the spread of the JTA across DoD functional domains and each Service's advocacy of its favoured standards and legacy system standards. The growth in the number of standards has the potential to turn the JTA into an architecture of multiple overlapping standards that threatens the JTA's interoperability goal.

---

[57] The US uses the word 'interoperability' in respect of systems owned by the USA while 'coalition connectivity' is the phrase that is used when the subject is US Forces working with coalition forces.

[58] *Report of the Defense Science Board Task Force on Tactical Battlefield Communications*, Washington DC, 17 February 2000 [unclassified report].

Canadian Ministry of Defence experience with C^3I Management

17. In the past the Department of National Defence and the Canadian Forces (DND/CF) experienced technical difficulties and delays with a number of their very large C^3I system projects.

18. DND/CF believes that its Defence strategy *Shaping the Future of Canadian Defence: A Strategy for 2020*[59] and its *Defence Planning Guidance 2000*[60] will improve C^3I interoperability between the Services. But much remains to be done. For many years the three Services maintained separate C^3I programs because their roles were separated by each Service's need to provide direct support to their sister Service in a NORAD and NATO context[61]. This did not produce high degrees of C^3I systems interoperability in Canada's defence force.

19. DND has appointed a Chief of Information Services to manage its administrative systems. Previously, IT systems were developed around functional group needs and this led to significant Information Management (IM) integration problems. The DND/CF sees that its goal of affordable and integrated IM systems depends on improved governance and having *one IM budget, one IM strategy, one architecture, one approach to C^4I and training and one set of expectations*. DND/CF is also seeking to avoid future large high-risk long-term projects by turning to evolutionary and modular approaches to system acquisition.

Conclusion

20. UK, US and Canadian defence organisations have responded to difficulties in achieving coherent and integrated information systems in two basic ways: by establishing a group responsible for knowledge system policy and development; and by establishing business processes that focus on managing operational, systems and technical elements. The aim is to allow systems related to the knowledge edge to evolve and be updated as coherently as practicable.

---

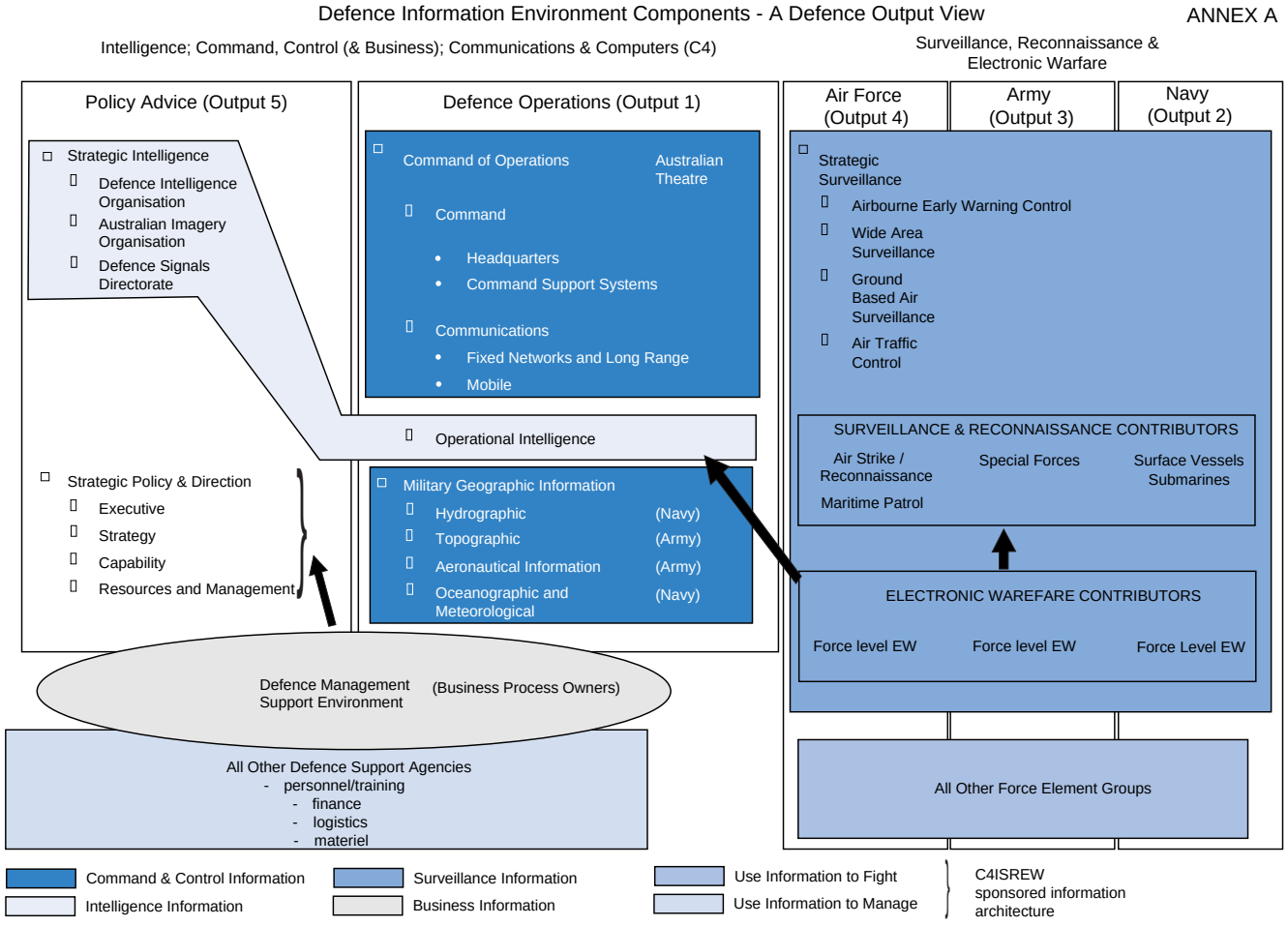
[59] Available: http://www.vcds.dnd.ca/cds/strategy2k/intro_e.asp [11 July 2000]

[60] Available: http://www.vcds.dnd.ca/dgsp/dpg/dpg2000/mess_e.asp [11 July 2000]

[61] NORAD: North American Aerospace Defense Command.
NATO: North American Treaty Organisation.

Appendix 4

Defence Information Environment—Outputs View



Source: Department of Defence

Appendix 5

Defence Outputs—May 2000

5 DEFENCE OUTPUTS	*Sub-outputs*	*Sub-sub-outputs*
1 Defence Operations		
1.1	Command of Operations	
	1.1.1	Command
	1.1.2	Communication
	1.1.3	Operational Intelligence
1.2	ADF Military Operations	
	1.2.1	Combat Operations
	1.2.2	Peacekeeping & Humanitarian Operations
1.3	Military Geographic Information	
	1.3.1	Hydrographic
	1.3.2	Topographic
	1.3.3	Aeronautical Information
	1.3.4	Oceanographic and Meteorological
1.4	International Relationships and Contribution to International Activities	
	1.4.1	International Engagement
1.5	Contribution to National Support Tasks	
	1.5.1	Emergency Management
	1.5.2	Defence Force Aid to the Civil Power
	1.5.3	Defence Force Aid to the Civil Community

continued next page

5 DEFENCE OUTPUTS	Sub-outputs	Sub-sub-outputs
2 Navy Capabilities		
2.1	Capability for Major Surface Combatant Operations	
2.2	Capability for Naval Aviation Operations	
2.3	Capability for Patrol Boat Operations	
2.4	Capability for Submarine Operations	
2.5	Capability for Afloat Support	
2.6	Capability for Mine Warfare	
2.7	Capability for Amphibious Lift	
3 Army Capabilities		
3.1	Capability for Special Forces Operations	
3.2	Capability for Mechanised Operations	
3.3	Capability for Light Infantry Operations	
3.4	Capability for Army Aviation Operations	
3.5	Capability for Combat Support to Land Forces	
	3.5.1	Ground Based Air Defence
	3.5.2	Capability for combat support of land operations
	3.5.3	Logistic Support
3.6	Capability for Motorised Infantry Operations	
3.7	Capability for Protective and Security Operations	

continued next page

5 DEFENCE OUTPUTS	*Sub-outputs*	*Sub-sub-outputs*
4 Air Force Capabilities		
4.1	Capability for Air Strike/Reconnaissance	
4.2	Capability for Tactical Fighter Operations	
	4.2.1	Lead In Fighter Operations
	4.2.2	Hornet/FAC Operations
4.3	Capability for Strategic Surveillance	
	4.3.1	Capability for Airborne Early Warning & Control
	4.3.2	Capability for Wide Area surveillance
	4.3.3	Capability for Deployable Ground Based Air Surveillance
	4.3.4	Capability for Air Traffic Control
4.4	Capability for maritime patrol aircraft operations	
4.5	Capability for Airlift	
	4.5.1	Light Tactical Airlift
	4.5.2	Medium Airlift
	4.5.3	Strategic Airlift
	4.5.4	VIP Transport
4.6	Capability for Combat Support of Air Operations	
	4.6.1	Capability for combat support of air operations
	4.6.2	Support Contingency Air Operations from Australia

continued next page

5 DEFENCE OUTPUTS	*Sub-outputs*	*Sub-sub-outputs*
5 Policy Advice		
5.1	Strategic Intelligence	
	5.1.1	DSD
	5.1.2	DIO
	5.1.3	DAIO
5.2	Strategic Policy and Direction	
	5.2.1	Executive
	5.2.2	Strategy
	5.2.3	Capability
	5.2.4	Resource & Management
5.3	International Policy	

Appendix 6

UK Defence Procurement Agency—Integration Authority

Integration Authority - in the UK Defence Procurement Agency

The Integration Authority is accountable to the Chief Executive of the Defence Procurement Agency (DPA) for the provision of advice on integration issues relating to the procurement of equipment. It is responsible for the development of a capability within the DPA to plan and manage the procurement of a "systems of systems" within an overarching systems integration architecture.

It will be answerable to Deputy Equipment Capability - Command Communications and Information Infrastructure (DEC CC&II), and thence to the Central Customer (Capability Managers, Capability Area Leaders and Capability Working Groups) for the provision of advice on integration issues relating to customer functions and for the application within the DPA of the environment for information coherence, supporting individual Integrated Project Teams (IPTs).

IT will be answerable to the Chief of Defence Logistics for the provision of advice on issues as they affect IPTs and equipment managed within the Defence Logistics Organisation. It will maintain a systems integration architecture which addresses the through life management and configuration of integrated systems that are in-service.

Source: Prepared by the ANAO from United Kingdom Ministry of Defence, *JSP 600 Pilot Version: The Environment for Information Coherence: A Manager's Guide*, v1.1, 1 December 1999, p.24.

.

Appendix 7

Standard Project Management Method Training Statistics

1. Standard Project Management Method (SPMM) training is progressing for project personnel from Defence Groups involved in major capital equipment acquisitions. The number of project management personnel trained in SPMM is shown in Table 3.

Table 3

Number of Defence officers trained in SPMM—January 1999 to May 2000

Group	DAO	ADHQ	SCA	Army	Navy	Not Known	Others	Total
Practitioner Trained	132	22	13	2	2	4	4	179
Overview Trained	260	60	10	7	6	12	15	370
Board Trained	19	13	5	2	5	5	5	54
Total	411	95	28	11	13	21	24	603

Source: Department of Defence
DAO — Defence Acquisition Organisation
ADHQ—Australian Defence Headquarters
SCA — Support Command Australia

2. The former Defence Acquisition Organisation (DAO) advised the ANAO that, in 1998, in addition to the numbers in Table 3, 250 staff in DAO, ADHQ and SCA were trained in SPMM and that approximately 60 DAO staff were also trained as a part of the PMM Rollout.[62]

3. Other statistics show that, by late in the audit, of the 1,383 personnel employed in Defence Materiel Organisation's (DMO's) project management branches, 492 had been trained in the SPMM and associated team training.[63] (DMO was formed recently by the merger of DAO and SCA.)

4. The number of personnel trained in DAO's Integrated Acquisition Team concepts is shown in Table 4.

Table 4

Number of Defence officers trained for Integrated Acquisition Teams

Group	DAO	ADHQ	SCA	DSTO	Total
Number Trained	103	25	24	25	177

Source: Department of Defence
DSTO—Defence Science and Technology Organisation

---

62 *BPRI Training Statistics*, BPRI Project Business Manager, E-mail of 15 May 2000.

63 Elizabeth Morse Consulting, *Report to Defence Acquisition Organisation on Training Needs Analysis,* Final Report, 27 June 2000, p.23.

Appendix 8

Secretary's Address on Knowledge Edge Management

This appendix sets out the edited text of an address by the Secretary of the Department of Defence, Dr Allan Hawke, on 25 August 2000.

IN SEARCH OF THE KNOWLEDGE EDGE

THE MANAGEMENT COMPONENT[64]

(Anecdote) That little story illustrates the Knowledge Edge—a concept based around people and knowledge management. People and information are key differentiators, critical to future success—in Defence and elsewhere.

I appreciate this opportunity to speak about our endeavours to improve Defence's knowledge management. I hope this will help you understand how CSC (and others) might align better with Defence's direction in this area.

We also need to recognise and accept change as a way of life—whether it be in Defence or in the broader market place, in which CSC is a major player. Those organisations not undergoing continuous renewal are going out of business—they're dying.

Defence's leadership is based on what we call a 'Results through People' approach. 'Results'—because, at the end of the day, that's what we're here to achieve on behalf of the Minister and the Government. 'People' -because results can come only through people—people are the key to superior performance. That's something we've lost sight of in some areas of Defence—a topic in its own right for another occasion.

The "Knowledge Edge" involves exploitation of information technologies and decision systems to maximise the effectiveness of our relatively small ADF. Our aim is for an integrated capability incorporating intelligence, communications, reconnaissance, surveillance, and the associated command support systems.

Organisations that rely for their competitive edge solely on technology or physical infrastructure delude themselves. Technology effectively applied is merely a potential multiplier—it's an enabler, not an end in itself. We are of the information age where software and hardware are

---

[64] Based on an address by the Secretary to CSC in the Great Hall, Parliament House, 25 August 2000.

easy to buy. Defence has been a dab hand at spending money in this way. In the end, it's how people use the technology that makes the difference.

Upon rejoining Defence, one of the things that dismayed me was the inability to send an e-mail to all of our people—CDF and I still can't do that!

Another was the lack of valid corporate information available to CDF, myself and other key decision-makers. For example, we can prove what's been saved under the Defence Review Program—we know those resources have been redeployed to the sharp end—but no one can tell us more precisely where those resources have gone to! This makes measuring our overall performance very difficult. It also creates significant credibility problems for us.

Presentations involving masses of data are commonplace, but converting them to valid and meaningful information to support decision making seems beyond us.

The search for a solution almost always focuses on the latest, most advanced technology as the panacea. That leads to another layer of technology, more data and, arguably, less information.

The technology solution leads inexorably to the technocrat's solution—in Defence we find it hard to learn the lessons of the past—we've developed stovepiped solutions to an art form. Stovepipes r us!

You might like to reflect on the fact that Defence now has

- **PMKEYS**—a People Soft personnel application;
- **ROMAN**—a SAP solution to facilitate financial management; and
- **SDSS**—a Mincom product to support our materiel function.

Each of these is, remarkably, based on a different chart of accounts! They can't, don't or won't talk to each other, other than under extreme duress through extraordinarily complicated interfaces and "hydraulics" at the end of the financial year. They even give us different answers to the same question—for example, the cost of personnel.

They can't, of course, coherently answer questions that would put us in danger of taking an informed business decision—eg how many people are involved in, and what is the cost of, any particular output or sub-output.

In other words, they are transaction processing systems that do not readily produce meaningful management information. The absence of a simple data dictionary compounds the problem of communication

between these corporate systems—each describes the same data differently and the apples with oranges comparison is the inevitable outcome.

Our Audit Committee, an essential part of our governance framework, has drawn my attention to these shortcomings in no uncertain terms. Having discussed the solution to the problem, the Chairman said "Well, if that's where you want to get to, I wouldn't start from where you are!" Their counsel was to fix the information gap and in parallel, put in train some much needed reforms on the financial management side.

That's not to decry the very significant advance of bringing together the many separate single service and civilian systems—a major and difficult task, in terms of sheer size and complexity. For example, PMKEYS required the translation of more than 100 separate systems into the one system. Separate systems often arise where centrally provided solutions are "manager hostile".

Even if each system was effective in its own right, they lack a clearly enunciated strategic framework in which to operate. Another problem relates to ownership (really lack of ownership) of the systems, the data input and the eventual outputs.

The move to accrual based output budgeting adds a new dimension, requiring us to integrate these separate systems to facilitate decision making. The reason we've got so many stand alone systems stems from the fact that the big systems don't do the job they're supposed to. This is also an elegant example of people doing their best to improve our performance. That requires attention to the lots of bad systems, processes and structures which frustrate that end.

And when you overlay that with cultural change you get some appreciation of the magnitude and complexity of the task.

Our IT solutions have too often reflected the way an individual unit performs its functions, but neglected the way our people act (or would like to act) between the various units within the organisation. A repeated cry, after a new IT solution has been implemented, is that the system is fine from the viewpoint of processing transactions, but it still does not provide the information needed to take daily decisions.

Plenty of promise—and promises for that matter—significant sunk cost, pretty poor performance. What do I mean by significant sunk cost?—probably in the order of 100s of millions of dollars over the last 10 years on the three principal systems alone. Yet more has been invested in the plethora of subordinate systems that have been developed to compensate for inadequacies in the principal systems.

Performance might best be illustrated by the fourth great lie "this hardware or software is fully IBM compatible".

That's a view from the top—it may be distorted, it may be unfair, but it is my perception.

What about the views of some of Defence's more experienced executives? I asked them about our future relationship. Three issues came to the fore:

- First, we mutually appear captive of the notion that "the system is the solution".
- Second, even when our IT requirement is clear, we find it difficult to specify in high level function and performance terms what we actually want. We work together to confound each other by quoting and contracting a hard-wired solution.
- Third, we have problems maintaining a cohesive team approach across the critical early phases of the project leading to less than desired performance in Project delivery to schedule, to budget, and to specified outcome.

Defence is data rich—information and knowledge poor.

How do we improve the information provided to our key decision makers? The information and knowledge often exists, but we don't group bits together or get them to where and when we need them. We revel in re-inventing the wheel, we're not particularly good at learning the lessons of our history, so our destiny seems rooted in repeating past mistakes, often with greater elan and effect.

That's the diagnosis, what's the solution?

Let me say a little about our approach to knowledge management—one aspect of our search for the knowledge edge.

Our mutual challenge may well be to achieve an environment where individuals are able to share experience; to learn from each other's successes and failures, and to make decisions on the basis of retained knowledge.

In "The Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation", Nonaka and Takeuchi outlined an approach for organisational management of knowledge—conversion of data and information into corporate knowledge—through continuous interaction of four elements:

- **Socialisation**—sharing information
- **Externalisation**—examining best practice as a catalyst for innovation—building conceptual knowledge
- **Combination**—synthesising information into a bigger and better combination—building systemic knowledge, and
- **Internalisation**—learning by doing—building operational knowledge.

Practitioners around the world regard those four elements as representing good knowledge management. Deep seated cultural changes are also needed to change the value systems and processes for effective knowledge management. As most CEOs know, cultural change is not affected with e-speed!

Our senior leadership recall day of 23 June featured an aspirational commitment to **"set the standard"**, something that Defence already does pretty well in some areas—e.g. warfighting skills, intelligence, science and technology.

Setting the standard will drive everything we do in Defence. You will appreciate the relationship between this and best practice. **Setting the standard** doesn't mean equalling or striving for best practice elsewhere—it means what it says, continuing to **set the standard** for best practice that others envy. That will require a lot of careful thinking and planning, plenty of elbow grease and work with companies like yours to this end.

On 23 June, the CDF and I also announced the creation of a Chief Knowledge Officer position. Air Vice Marshal Peter Nicholson became the CKO having previously enjoyed the remarkable title of HC4ISREW, known colloquially as head screw. He becomes the strategic director of Defence business systems and knowledge development aspects. I expect him to look at this from an executive management decision-support viewpoint.

In what some may regard as an heretical approach, his priority task is to develop a Defence Enterprise Architecture. To borrow from VCDF's riding instructions, we are alert to the danger of this becoming an exercise characterised by extreme levels of activity, endless debate and negligible results. We expect Peter's report to reflect Charles Dickens' style rather than esoteric cyber language. Having said that, VCDF had "Great Expectations" in mind rather than "Bleak House" or "The Mystery of Edwin Drood".

One of my spiritual advisers has counselled me that Australians don't like to fail. I fear that the arduous nature and enormity of the task that

we've set for the CKO may be an impossible ask for any individual. Peter will need external and internal assistance to achieve our goal.

Defence has made some knowledge management progress in its enterprise-level IT infrastructure development—currently the province of Patrick Hannan, who I see as the Chief Information Officer. The Information Systems Group it has provided a sound foundation in Web-based technologies—both internet and intranet—something not well appreciated by others. I suspect they (DISG) would add that the challenge of managing something that has an exponential growth curve is not to be underestimated and is even less well appreciated.

We have an evolving national IT infrastructure, and are working to achieve an environment which performs consistently across Defence—across our 50,000 or so desktops. We have the basis for building our shared and conceptual knowledge—we just don't do much of either.

The problems of combining data and information in military and administrative environments is appreciated—our systemic knowledge is not good. The ability of the ADF's tactical platforms and surveillance systems to exchange key operational information is also less than desired.

We are serious about increasing our corporate knowledge capital. The ANAO recently reminded us of immediate areas of focus:

- greatly improving the coherence of our underlying core business processes to improve Defence's Information Environment;
- serious data warehousing—linking our three stovepipes to build real systemic knowledge;
- rationalising the literally 100s of 2nd—and 3rd—level information systems that soak up lots of support resources while contributing little or nothing to our knowledge capital and corporate decision-making abilities;
- encouraging individual and group behaviour to focus on information sharing; combining information and knowledge; and on learning and applying across Defence the processes we individually know to be successful; and
- integrating processes, tools and data to build Defence's knowledge base.

I interpret these ANAO remarks as five action statements. Geoff Davis will be leading a team to tackle these issues. His plan of attack is due with me and the Minister by the end of the month. If you didn't appreciate the subtlety of what I just said—this is clearly a "watch this space" announcement with significant Ministerial clout behind it!

We won't achieve our goals by working alone. My views on knowledge management implicitly include significant industry support for our efforts. You might like to consider how a company like CSC—the breadth and depth of talent in this room—can add real value to Defence's knowledge management challenges—on the people as well as the system sides.

The challenge is on your table as well as mine, and the potential benefits are enormous. Obtaining the "Knowledge Edge" will allow our people to achieve results beyond our "fighting weight". It's time to solve Defence's knowledge management problem!

Appendix 9

Performance audits in Defence

Set out below are the titles of the ANAO's previous performance audit reports on the Department of Defence and the Australian Defence Force (ADF) tabled in the Parliament in the last five years.

Audit Report No.8 1995–96
Explosive Ordnance (follow-up audit)

Audit Report No.11 1995–96
Management Audit

Audit Report No.17 1995–96
Management of ADF Preparedness

Audit Report No.26 1995–96
Defence Export Facilitation and Control

Audit Report No.28 1995–96
Jindalee Operational Radar Network Project [JORN]

Audit Report No.31 1995–96
Environmental Management of Commonwealth Land

Audit Report No.15 1996–97
Food Provisioning in the ADF

Audit Report No.17 1996–97
Workforce Planning in the ADF

Audit Report No.27 1996–97
Army Presence in the North

Audit Report No.34 1996–97
ADF Health Services

Audit Report No.5 1997–98
Performance Management of Defence Inventory

Audit Report No.34 1997–98
New Submarine Project

Audit Report No.43 1997–98
Life-cycle Costing in Defence

Audit Report No.2 1998–99
Commercial Support Program

Audit Report No.17 1998–99
Acquisition of Aerospace Simulators

Audit Report No.41 1998–99
General Service Vehicle Fleet

Audit Report No.44 1998–99
Naval Aviation Force

Audit Report No.46 1998–99
Redress of Grievances in the ADF

Audit Report No.13 1999–00
Management of Major Equipment Acquisition Projects

Audit Report No.26 1999–00
Army Individual Readiness Notice

Audit Report No.35 1999–00
Retention of Military Personnel

Audit Report No.37 1999–00
Defence Estate Project Delivery

Audit Report No.40 1999–00
Tactical Fighter Operations

Audit Report No.41 1999–00
Commonwealth Emergency Management Arrangements

Audit Report No.50 1999–00
Management Audit Branch—Follow-up

Audit Report No.3 2000–01
Environmental Management of Commonwealth Land—follow-up

Audit Report No.8 2000–01
Amphibious Transport Ship Project

Glossary

Architecture: *"The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time". "Organisational structure of a system or component".* [IEEE STD 610.12, via TAF1M V3.0 Draft]

Command: Command in the general sense is defined as:

> *the authority which a commander in the military Service lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organising, directing coordinating and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale and discipline of assigned personnel [Chapter 7: Command and Control of Australian Defence Force Operations* (ADFP 1: Doctrine), 30 November 1993] [STRATCONCEPT C3]]

Control: Control is the mechanism by which command is implemented. Control of implementation includes monitoring and reassigning by originating authorities to ensure successful outcomes in terms of effectiveness and efficiency. An important part of control is coordination which is defined as, the bringing of objects together so that they can cooperate in carrying out a process. It includes the coordination of planning and decision-making to maximise the utility of limited resources. [STRATCONCEPT C3)

Control includes both: the translation, by staff, of commanders' directives into an implementation *plan*, based on, *inter alia*, the commander's intent, knowledge and assessment of the situation, his assigned resources and his mission; and the subsequent monitoring of the conduct of the resultant operation so that the necessary corrective actions may be taken to either realign forces with the commander's directives or identify and take up new opportunities. In short, *control is primarily about the management of operations.* The main "products" of "control" are plans, orders, tasking etc and situation reports. [Dr Vic Sobolewski, (Draft) Appendix A to ADF C31 Force Development Process, 1996]

Evolutionary Acquisition (EA): The incremental specification, design, implementation, testing, delivery, operation and maintenance of systems. The delivery of each incremental release increases the overall capability of the system until it is complete. In this way users of the system get early access to functionality and are encouraged to provide feedback on

functionality and performance. The feedback is used in subsequent increments to shape the development of the system as it evolves to its final form. [Derek Henderson, *Evolutionary Acquisition of Battlefield Command Systems*, DSTO, 1999, p.1]

Framework: "*A structure of element types to which specific instances may be attributed to define an architecture*." [DIAG discussion]

Information Management: The management of *information systems* to ensure the effective and efficient handling of *information to* achieve corporate goals. Knowledge Management subsumes Information Management.

Information Systems: The *combination of* resources (including information technology and people) required to handle and process the included information for a specific purpose.

Information Technology: The *components and* mechanisms for handling and processing information.

Infrastructure: That set of elements that comprise a basis for the provision of services or functions. [DIAG Discussion]

Integration: The merging of disparate systems into a single logical system through commonality of architectures, data structures or definitions, application software, operating systems, hardware, procedures and doctrine.' [ADF Command & Control Information Systems Plan (CCISP) 199516 (Issue 1.0)]

Interoperability: "*is the ability of systems, units or forces to provide services to, and accept services from, other systems, units or forces and to use the exchanged services to operate effectively together without altering or degrading the information exchanged*." [ADF Command & Control Information Systems Plan (CCISP) 1995 (Issue 1.0)]

Joint: (NATO) Connotes activities, operations, organisations, etc in which elements of more than one Service of the same nation participate. (When all Services are not involved, the participating Services shall be identified, eg. Joint Army–Navy). [Chapter 10: Glossary (ADFP 101: Glossary)]

Knowledge Management: "*Knowledge Management is the explicit control and management of knowledge within the organisation aimed at achieving the organisations objectives. It aims to improve the performance of processes, organisations and systems from the perspective that knowledge is thereby the crucial production factor.*" [Gardner, K. (1995). Position paper for the International Knowledge Management Congress]

Legacy Application: *'an application that, under either a broader emerging set of system requirements or an altered set of constraints, is deemed to no longer closely fit the current business model.'* [DIAG]

System: "*People, machines and methods organised to accomplish a set of specific functions.*" [TAF1M V3.0 Draft derived from FIPS Pub 11–3]

Tactical Command: (NATO) The authority delegated to a commander to assign tasks to forces under his command for the accomplishment of the mission assigned by higher authority. [Chapter 20: Glossary T (ADFP 101: Glossary)]

Tactical Control: "*detailed and, usually, local direction and control of movements or manoeuvres necessary to accomplish missions or tasks assigned*". [Chapter 7: Command and Control of Australian Defence Force Operations (ADFP 1: Doctrine), 30 November 1993]

Index

Series Titles

Titles published during the financial year 2000–01

Audit Report No.9 Performance Audit
Implementation of Whole-of-Government Information Technology Infrastructure Consolidation and Outsourcing Initiative

Audit Report No.8 Performance Audit
Amphibious Transport Ship Project
Department of Defence

Audit Report No.7 Performance Audit
The Australian Taxation Office's Use of AUSTRAC Data
The Australian Taxation Office

Audit Report No.6 Performance Report
Fraud Control Arrangements in the Department of Health & Aged Care
Department of Health & Aged Care

Audit Report No.5 Performance Report
Fraud Control Arrangements in the Department of Industry, Science & Resources
Department of Industry, Science & Resources

Audit Report No.4 Activity Report
Audit Activity Report: January to June 2000—Summary of Outcomes

Audit Report No.3 Performance Audit
Environmental Management of Commonwealth Land—Follow-up audit
Department of Defence

Audit Report No.2 Performance Audit
Drug Evaluation by the Therapeutic Goods Administration—Follow-up audit
Department of Health and Aged Care
Therapeutic Goods Administration

Audit Report No.1 Performance Audit
Commonwealth Assistance to the Agrifood Industry

Better Practice Guides

AMODEL Illustrative Financial Statements 2000	Apr 2000
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building a Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No.47 1998–99)	Jun 1999
Commonwealth Agency Energy Management	Jun 1999
Corporate Governance in Commonwealth Authorities and Companies–Principles and Better Practices	Jun 1999
Managing Parliamentary Workflow	Jun 1999
Cash Management	Mar 1999
Management of Occupational Stress in Commonwealth Agencies	Dec 1998
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	Jul 1998
Life-cycle Costing (in Audit Report No.43 1997–98)	May 1998
Controlling Performance and Outcomes	Dec 1997
Management of Accounts Receivable	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997
Public Sector Travel	Dec 1997
Audit Committees	Jul 1997
Core Public Sector Corporate Governance (includes Applying Principles and Practice of Corporate Governance in Budget Funded Agencies)	Jun 1997
Administration of Grants	May 1997
Management of Corporate Sponsorship	Apr 1997
Return to Work: Workers Compensation Case Management	Dec 1996
Telephone Call Centres	Dec 1996
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Performance Information Principles	Nov 1996
Asset Management	Jun 1996
Asset Management Handbook	Jun 1996
Managing APS Staff Reductions	Jun 1996