Australian Government
Department of Defence
Defence Science and
Technology Organisation

A Review of Enterprise Architecture Use in Defence

Meredith Hue

Defence Systems Integration Technical Advisory
Joint and Operations Analysis Division
Defence Science and Technology Organisation

DSTO-TR-3040

ABSTRACT

This report provides a retrospective analysis of enterprise architecture practice in Defence over the last decade leading to the establishment of the Integrated Defence Architecture. A review was undertaken to gain insight into the perceived value that various Stakeholders within Defence were realising from the use of enterprise architectures to assist with the realisation of the integrated networked force. The report distils lesson learned over this period and provides a benchmark to evaluate the effectiveness of subsequent enterprise architecture practice in Defence. The impetus for enterprise architectures and the modus operandi were also examined to provide context to the review findings.

RELEASE LIMITATION

Approved for Public Release

Published by
Defence Systems Integration Technical Advisory
Joint and Operations Analysis Division
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: 1300 333 362
Fax: (08) 7389 6567

AR-016-127
September 2014

APPROVED FOR PUBLIC RELEASE

A Review of Enterprise Architecture Use in Defence

Executive Summary

The Department of Defence has embraced the notion of enterprise architecture not only as a means of achieving significant ICT reform, but also to assist with the realisation of the integrated and networked Future Joint Force of 2030.

This report provides a retrospective of enterprise architecture practice in Defence over the last decade leading to the establishment of the Integrated Defence Architecture. The report distils lessons learned over this period and provides a benchmark to evaluate the effectiveness of future enterprise architecture practice in Defence.

A review was undertaken on behalf of the Chief Systems Integration Officer (CSIO) to examine specific enterprise architecture initiatives since the release of the Defence White Paper 2009 towards establishing the Integrated Defence Architecture.

Two central questions were posed to interviewees:

1. What value are you getting from architectures?
2. Is it providing you with the answers you need?

A sampling of key stakeholders revealed a number of concerns relating to the implementation of enterprise architecture practice over the period of examination. Expression of these concerns was consistent across different stakeholder groups across Defence:

1. None of the respondents from CDG, DMO, VCDF and the Services indicated they were getting value from the extant architecting effort in Defence within the Warfighter IDA sub-domain.
2. None of these respondents indicated they were getting the answers they needed from the extant enterprise architecture effort in Defence.

Concerns of users included the perceptions expressed as follows:

1. Architecting effort was not being directed to address user needs;
2. There was no formalised methodology provided for analysis and production of architectural information;
3. There were significant issues with data validation and management limiting the usability and hence utility of architectural information;
4. There were significant issues with levels of stakeholder resourcing to support IDA architecting activity;
5. There were significant issues with governance, where the endorsement and review process for architectural information was not clear;
6. There were significant issues with training of Defence personnel in enterprise architecture practice and retaining corporate memory.

The following insights were revealed:

1. There was widespread disparity about the meaning, applicability, purpose, methodology and resourcing of enterprise architecture practice in Government and Defence;
2. Significant reliance was placed on individual points of contact within Defence to provide guidance and advice on enterprise architecture policy and IDA implementation rather than utilising publications;
3. Linkages between different organisational enterprise architecture initiatives were not explicit so it was difficult to establish the existence of various policy initiatives;
4. There was little consistency in application of enterprise architecture principles across the various bodies of work undertaken under the auspices of the IDA;
5. Significant effort was expended towards documenting extant infrastructure and processes rather than providing guidance for future investment and process change;
6. The applicability of enterprise architecture policy directives and recommended enterprise architecture practice for DCP projects was inconsistent with other capability development process and governance mandates, and with systems engineering precepts; and
7. Particularly for the warfighter domain, enterprise architect concepts were being applied for specialised system developments that were inherently not enterprise-wide. The initial IDA approach lacked the formalisms and processes required to provide the necessary detail and rigour to manage implementation of specialised capability systems.

Numerous problems were evident with the enterprise architecture approach, which sought to develop a uniform ICT environment spanning whole-of-Defence to reduce costs and increase efficiency, but against the backdrop of multiple and overlapping governance frameworks, conflicting requirements, and disparate priorities.

The imposition of large-scale, standardised corporate solutions in the warfighting environment without consideration of the suitability and limitations within the specific threat environment and physical environment context was also ill-advised.

The following recommendations are offered:

1. To clarify and explicitly articulate from a whole-of-Defence perspective:
   - What are the meaning, scope, applicability, intent and limitations of Defence enterprise architecture practice?
   - What are the implications of whole-of-government enterprise architecture guidance and how are these to be reconciled in the Defence context?
   - How should enterprise architecture practice to be implemented, in terms of methodologies, technical and management processes, and governance?
   - How does enterprise architecture relate to other Defence technical and management processes?
   - Who should be involved and in what way, in terms of roles, responsibilities, contributions, end-usage and beneficiaries?

2. To clarify and explicitly articulate how the IDA and its accompanying enterprise architecture effort can provide utility in support of the capability development process over the entire capability life cycle.

3. To establish and manage an accessible and readily navigable information repository.

4. To enhance the stakeholder consultation process to ensure appropriate feedback is obtained and followed through, to the satisfaction of the parties concerned.

5. To enhance governance mechanisms to assure:
   - the integrity of architectural information and its suitability for the intended usage;
   - the appropriate guidance is provided to stakeholders; and
   - the appropriate authorities are enforced.

6. To develop an appropriately skilled workforce, with ready access to suitable training courses, training material, and tools, which reflect the specific intent and usage in the Australian Defence context.

7. To implement an evaluation process that monitors and reports on the progress of reforms to facilitate improved utility of enterprise architecture effort.

Further enquiry is also recommended to:

- Examine the range and nature of architectural information being generated across Defence to identify criteria to discern which information is architecturally significant from a whole-of-Defence perspective.
  - for example, distilling those systems or components, characteristics, and/or relationships that have broader organisational impact and therefore may be candidates for further standardisation on a larger scale.
- Examine possible Measures of Performance and Measures of Effectiveness for the significant architectural elements, and possible methods for performance monitoring.
- Examine the potential of OR and systems engineering methodologies to undertake analyses to support the EA outcomes sought to value-add to other forms of enquiry.
- Examine methods for more effective promulgation and governance of enterprise architecture-related matters to the broader stakeholder community.

Author

Meredith Hue
Defence Systems Integration Technical Advisory
Joint and Operations Analysis Division

Meredith is responsible for providing advice on defence systems integration principles and practices targeting systemic problems in Defence, and working with projects to address specific system integration issues. A former Chief Engineer, she has over 35 years experience in both Industry and Defence as a Systems Engineering practitioner, in the areas of real-time systems, combat systems and military communications. Specific interests include Systems, Systems of Systems, Enterprise Architecting, and Systems Architecting methodologies supporting capability development, including modelling and analysis of C4ISR architectures.

Contents

Abbreviations and Acronyms

ACCS	Australian Capability Context Scenarios
ACR	Architecture Compliance Review
ADDP	Australian Defence Doctrinal Publication
ADFA	Australian Defence Force Academy
ADFP	Australian Defence Force Publication
ADF	Australian Defence Force
ADL	Architecture Description Language
ADO	Australian Defence Organisation
AGA	Australian Government Architecture
AGAF	Australian Government Architecture Framework
AGIMO	Australian Government Information Management Office
AMD	Australian Maritime Doctrine
API	Application Program Interface
APL	Approved Products List
ARB	Architecture Review Board
ARM	Architecture Review Meeting
ATSL	Australian Technical Standards List
AUSDAF	Australian Defence Architecture Framework (also known as DAF)
AWG	Architecture Working Group
BABOK	Business Analysis Body of Knowledge
BCS(L)	Battlespace Communication System (Land)
BCSS	Battlespace Command Support System
BOK	Body of Knowledge
BPM	Business Process Modelling
BRM	Business Reference Model
BTIA	Battlespace Tactical Information Architecture
CAF	Chief of Air Force
CD	Compact Disk
CDD	Capability Development Documentation
CDF	Chief of the Defence Force
CDG	Capability Development Group
CIO	Chief Information Officer
CIOG	Chief Information Officer Group
CIS	Communications and Information Systems
CM	Capability Manager
COE	Common Operating Environment
CoI	Community of Interest
COP	Common Operating Picture
COTS	Commercial-off-the-Shelf
CPD	Capability Planning Directive
CSIO	Chief Systems Integration Officer
DAF	Defence Architecture Framework (also known as AUSDAF)
DARS	Defence Architecture Repository System

DAT	Defence Application Taxonomy
DCA	Defence Corporate Architecture
DCDH	Defence Capability Development Handbook
DCP	Defence Capability Plan
DEA	Defence Enterprise Architecture
DEAC	Defence Enterprise Architecture Committee
DEAP	Directorate of Enterprise Architecture Practice
DEAWG	Defence Enterprise Architecture Working Group
DIE	Defence Information Environment
DIEP	Defence International Engagement Plan
DI(G)	Defence Instruction (General)
DII	Defence Information Infrastructure
DMO	Defence Materiel Organisation
DoDAF	Department of Defense Architecture Framework (U.S.)
DPG	Defence Planning Guidance
DRM	Data Reference Model
DSG	Defence Support Group
DSM	Defence Security Manual
DSMS	Defence Standards Management System
DSTO	Defence Science Technology Organisation
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
EIA	Electronic Industries Alliance (known as Electronic Industries Association prior to 1997)
EPL	Evaluated Products List
ESB	Enterprise Service Bus
FASOC	Future Air and Space Operating Concept
FEA	Federal Enterprise Architecture (U.S.)
FEAF	Federal Enterprise Architecture Framework (U.S.)
FIC	Fundamental Inputs to Capability
FJOC	Future Joint Operating Concept
FLOC	Future Land Operating Concept
FMOC	Future Maritime Operating Concept
FPS	Function and Performance Specification
FSR	Force Structure Review
GEA	Gartner Enterprise Architecture
HR	Human Resource
ICT	Information and Communications Technology
IDA	Integrated Defence Architecture
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronic Engineering
INCOSE	International Council on Systems Engineering
IPT	Integrated Project Team
ISO	International Standards Organisation
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JCSE	Joint Command Support Environment

JIA	Joint Intelligence Architecture
JOA	Joint Operations Architecture
JOCOPR	Joint Operations Command Operational Preparedness Directive
MBSE	Model-based Systems Engineering
MILIS	Military Integrated Logistics Information System
MIS	Management Information System
MODAF	Ministry of Defence Architecture Framework (UK)
NBA	Networked Battlespace Architecture
NBA 2020+	Networked Battlespace Architecture 2020+
NCW	Network Centric Warfare
NDES	National Defence Estate Strategy
NEAF	Navy Enterprise Architecture Framework
NIE	Navy Information Environment
NIEP	Navy International Engagement Plan
OCD	Operational Concept Document
OGO	Other Government Organisations
OMG	Object Management Group
OR	Operations Research
PMBOK	Project Management Body of Knowledge
PRM	Performance Reference Model
QSR	Quarterly Strategic Review
RFT	Request for Tender
SAP	Systemanalayse und Programmentwicklung
SEBoK	Systems Engineering Body of Knowledge
SEP	Systems Engineering Process
SIE	Single Information Environment
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SOE	Standard Operating Environment
SRM	Service Reference Model
SRP	Strategic Reform Program
SW	Software
SWEBOK	Software Engineering Body of Knowledge
TCD	Test Concept Document
TIED	Tactical Information Interchange Domain
TOGAF®	The Open Group Architecture Framework
TOR	Terms of Reference
TRM	Technical Reference Model
U.S.	United States of America
US DoD	United States Department of Defense
VCDF	Vice Chief of the Defence Force.
ZF	Zachman Framework for Enterprise Architecture

This page is intentionally blank

1. Introduction

Considerable effort has been expended over the last decade on enterprise architecture (EA) related activity to assist delivery of Defence information and communications technology (ICT) related capability. This effort escalated with the release of the 2009 Defence White Paper. The Department of Defence has embraced the notion of EA not only as a means of achieving significant ICT reform, but also to assist with the realisation of the integrated and networked Future Joint Force of 2030 (DWP 2009). This report provides a retrospective analysis of enterprise architecture practice in Defence over the last decade leading to the establishment of the Integrated Defence Architecture. The report distils lessons learned over this period and provides a benchmark to evaluate the effectiveness of subsequent enterprise architecture practice in Defence.

A review was undertaken on behalf of the Chief Systems Integration Officer (CSIO) to examine specific EA initiatives and EA practice subsequent to the release of the Defence White Paper 2009. The review sought to gain insight into the perceived value that various stakeholders within Defence were realising from the use of EA to assist with the realisation of the Future Joint Force of 2030. This report documents the findings of the review and provides recommendations to respond to the findings. The impetus for EA and modus operandi were also examined to provide context to the review findings. The outputs of the review provide a snapshot of the state of EA practice in Defence and reflect on perceived stakeholder community utility and value of EA in Defence over the period of examination.

2. Methodology

2.1 Stakeholder Selection

A number of key stakeholders were selected across a broad range of Defence organisations and responsibilities contributing to Defence capability development.

Stakeholders were selected for interview from VCDF, DMO, Capability Managers (CMs), CIOG and CDG personnel within the Defence EA Community of Interest (CoI). A list of Stakeholders consulted is provided in Section 10.

Stakeholder views were solicited via a series of informal interviews using directed questioning technique with open questions. Interviewees were also invited to contribute additional comment to elaborate or clarify their particular perspective.

EA-related material was reviewed and a number of CIOG-initiated Defence Enterprise Architecture Working Group (DEAWG) meetings were attended. CIOG-initiated Architecture Working Group (AWG) meetings and Architecture Review meetings (ARM) were also attended for various in-house projects, including:

- DeBI – Defence eBusiness Initiative
  - CIOG-led project to implement Enterprise Service Bus (ESB) and Enterprise Application Integration Infrastructure using Service-Oriented Architecture (SOA) concepts.
  - Integration Infrastructure described the envisaged capabilities that would enable applications that run on different platforms and devices or written in different languages and models with different data structures to communicate and/or integrate.
  - Implemented two specific application integration architectural patterns: Request Reply and File Transfer patterns;
- eHealth - Joint eHealth Data Information System[1]
  - Vision was to provide one electronic health record for Australian Defence Force (ADF) personnel, from recruitment to discharge, then through management in other agencies.
  - RPDE investigated commercial-off-the-shelf (COTS) eHealth products to provide a fast-track interim solution to address the lack of a comprehensive health information system.
- StratCOP – Strategic Common Operating Picture Compilation and Distribution
  - RPDE Task 38 investigated COTS products to assemble and distribute a Strategic Common Operating Picture (COP) for viewing on a Defence fixed network.
- AUSDAF2 – Defence Architecture Framework Version 2[2]

[1] [online] URL : http://intranet.defence.gov.au/vcdf/sites/JeHDI/ComWeb.asp?page=82815
[2] [online] URL : http://ciogintranet/organisation/CTOD/ICTSAB/Pages/Directorate%20of%20Enterprise%20Architecture%20Practice.aspx

  - CIOG-led project to update the Defence Architecture Framework to incorporate additional views and viewpoints to support Defence's enterprise architecture effort.

- BTIA – Battlespace Tactical Information Architecture[3]
  - CIOG-led project to develop an architecture guidebook and a set of DAF views to describe the Battlespace Tactical Information Architecture (BTIA).
- GEMS – Garrison and Estate Management System[4]
  - Defence Support Group led project to provide an enabler for generational change in Estate Management.
  - Aim was to provide a centralised Defence garrison and estate management system.
  - To be implemented as part of an extended Defence SAP environment
    - SAP is a modular enterprise level financial and resource planning software suite, originally known as "Systemanalayse und Programmentwicklung" (SAP).

Desk officers and Integrated Project Team (IPT) members were interviewed and/or material reviewed associated with a number of DCP projects with significant Information and Communications Technology (ICT) content including[5]:

- JP 2089 - Tactical Information Interchange Domain (TIED);
- SEA 1442 - Maritime Communications Modernisation;
- JP 2072 – Battlespace Communications System Land (BCS(L));
- JP 2030 – Joint Command Support Environment (JCSE);
- Land 125 – Soldier Combat System;
- Land 75 – Battlefield Command Support System (BCSS); and
- JP 2077 – Military Integrated Logistics Information System (MILIS).

Capability Managers (CM) were interviewed from all three Services: Army, Navy, and Air Force, as well as Joint.

Since value and utility are context dependent, no specific definitions were employed; the different perspectives were recounted from the respective interviewees instead.

2.2 Information Sought

Two central questions were posed to the interviewees:

1. What value are you getting from architectures?
2. Is it providing you with the answers you need?

---

[3] [online] URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/Warfighter%20(NBA%202020).aspx

[4] [online] URL : http://intranet.defence.gov.au/dsg/sites/GEMS/ComWeb.asp?page=84147

[5] Information on the respective DCP projects can be found on the DMO website at URL: http://intranet.defence.gov.au/dmoweb/sites/_Home/comweb.asp?page=91637.

To help frame the responses in the appropriate context, the following information was elicited from those stakeholders in Defence who were involved with developing or using architectures:

- What do you understand by the term designing/architecture practice?
- Why are architectures relevant to you?
- What questions are you are asking?
- Who does the designing?
- Why are they designing?
- What relevant experience or expertise do they have?
- What training have they received, and who from?
- What tools do they use?
- What level of effort/resources (people, hours) has been applied?
- What is the nature and scope of the problem to be architected?
- What is the output going to be used for?
- Who is the output being provided to?
- Who else has access to the output?
- Have architectures been useful to you?
- What issues or challenges have you encountered, and what have been the consequences?
- To what time frame does this information relate?
- Are you satisfied that the resources you have used have given you commensurate value?

3. Background Influences – Capability Planning

3.1 Defence Strategy Planning Guidance

The Defence White Paper is a key source for capability planning guidance of Defence. The 2009 White Paper "*Defending Australia in the Asia Pacific Century: Force 2030*" and its companion White Paper 2013 update laid out the Government's future plans for Defence to achieve the future ADF over the period to 2030. They also describe how those plans would be achieved through directing major Defence capability investment, to ensure the funding was "well targeted and well managed to get the right Defence capability at the right cost" (DWP 2009 pg 138).

A Strategic Reform Program (SRP) was initiated subsequent to the White Paper 2009 to provide a Defence-wide effort to create the structure and processes to enable Defence to meet the White Paper 2009 objectives effectively and efficiently (SF 2010), (SRP 2010).

The *Strategy Framework 2010* is another key document linked to the White Paper, aiming to synchronise the formulation of strategic guidance and strategic planning, including capability development effort, across whole-of-Defence. The Strategy Framework provided guidance to the set of documents that comprised Defence's strategic planning at that time, including the relationships between these documents as shown in Figure 1.

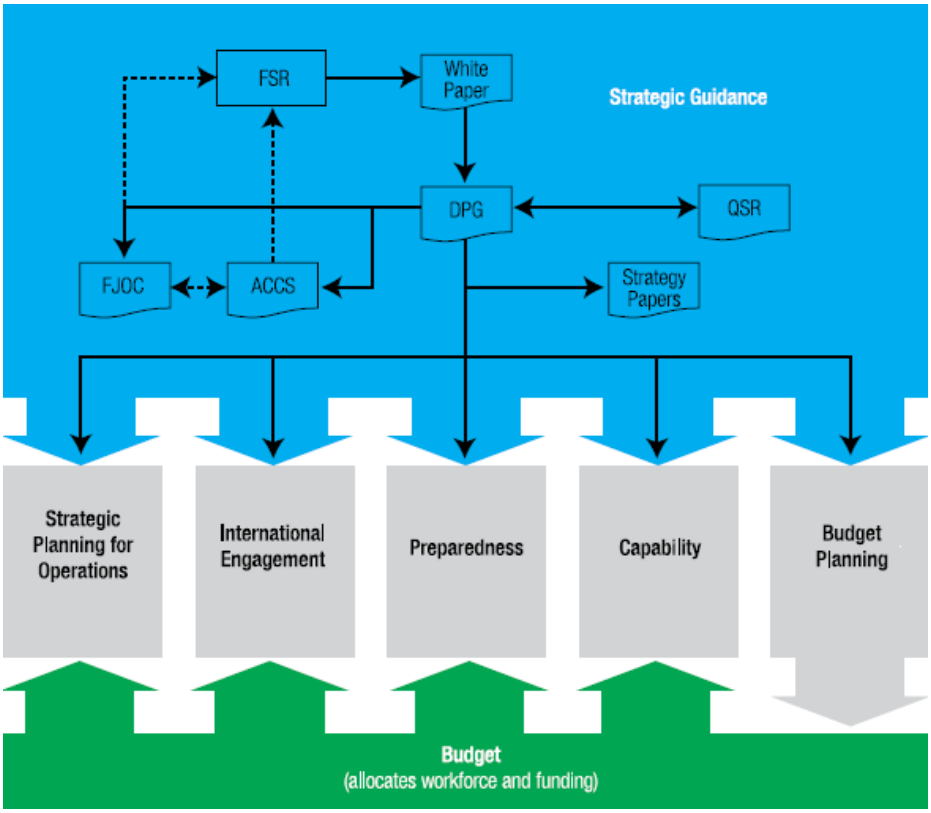


Figure 1 *Key Strategy Framework Guidance and Influences (SF 2010).*

Key output products and documents synchronised within the auspices of the Strategy Framework are described in Table 1:

Table 1 Key Strategy Framework Products and Strategy Documents (SF 2010).

Strategy Framework Product Descriptions	***Service-Level Strategy Documents***
Defence White Paper (DWP)	Australian Maritime Doctrine (AMD)
Defence Planning Guidance (DPG)	Future Maritime Operating Concept (FMOC)
Quarterly Strategic Review (QSR)	Navy Strategic Plan
Australian Capability Context Scenarios (ACCS)	Navy International Engagement Plan (NIEP)
Foundations of Australian Military doctrine (APDD-D)	Adaptive Army
Future Joint Operating Concept (FJOC)	Chief of Army's Strategic Guidance for Land Force
CDF Planning Directives	Adaptive Campaigning – Future Land Operating Concept (FLOC)
Defence International Engagement Plan (DIEP)	Chief of Army's Preparedness Directive
CDF Preparedness Directive (CPD)	Army International Engagement Plan
Joint Operations Command Operational Preparedness Requirement (JOCOPR)	Future Air and Space Operating concept (FASOC)
Defence Capability Plan (DCP)	Air Force Plan
Defence Strategic Workshop Plan (DSWP)	CAF Capability Intent
National Defence Estate Strategy (NDES)	Air Force International Engagement Strategy

3.2 Defence Capability Planning Guidance

Government top-level priorities for capability development are developed and promulgated through the Defence White Paper and Defence Planning Guidance as shown in Figure 2.

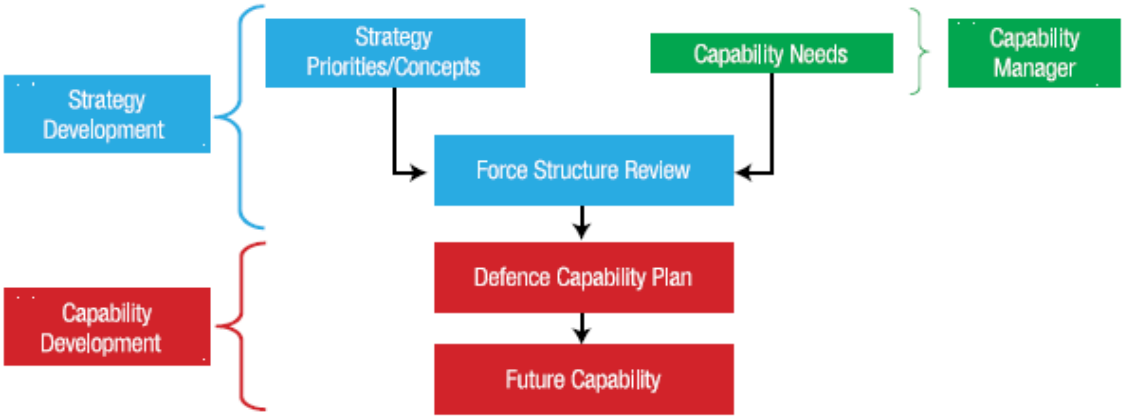


Figure 2 Key Capability Planning Influences and Responsibilities (SF 2010).

The DCP is the key planning document guiding acquisition of new Defence capability towards realisation of the future joint force of ADF 2030 (DCP 2012). This plan is the Major Capital Investment Program for Defence, and is managed as a portfolio of projects.

Defence has a maturing capability development process drawing from systems engineering principles as described in the *Defence Capability Development Handbook 2012* (DCDH 2012). The principle aim of capability development is to develop and maintain the most operationally effective and cost-efficient mix of Defence capabilities to achieve the Australian Government's strategic objectives (DCDH 2012).

The Defence capability development process as detailed in (DCDH 2012) describes the primary process mechanisms and governance requirements for acquiring and evolving Defence capability within the Department of Defence. A capability life cycle is ascribed to each capability system as shown in Figure 4 to visualise the life of the capability system from the identification of a need (i.e. an existing or emerging Defence capability gap) through to the acquisition of a physical capability system, which is operated and supported over the life of the capability system until its eventual disposal.

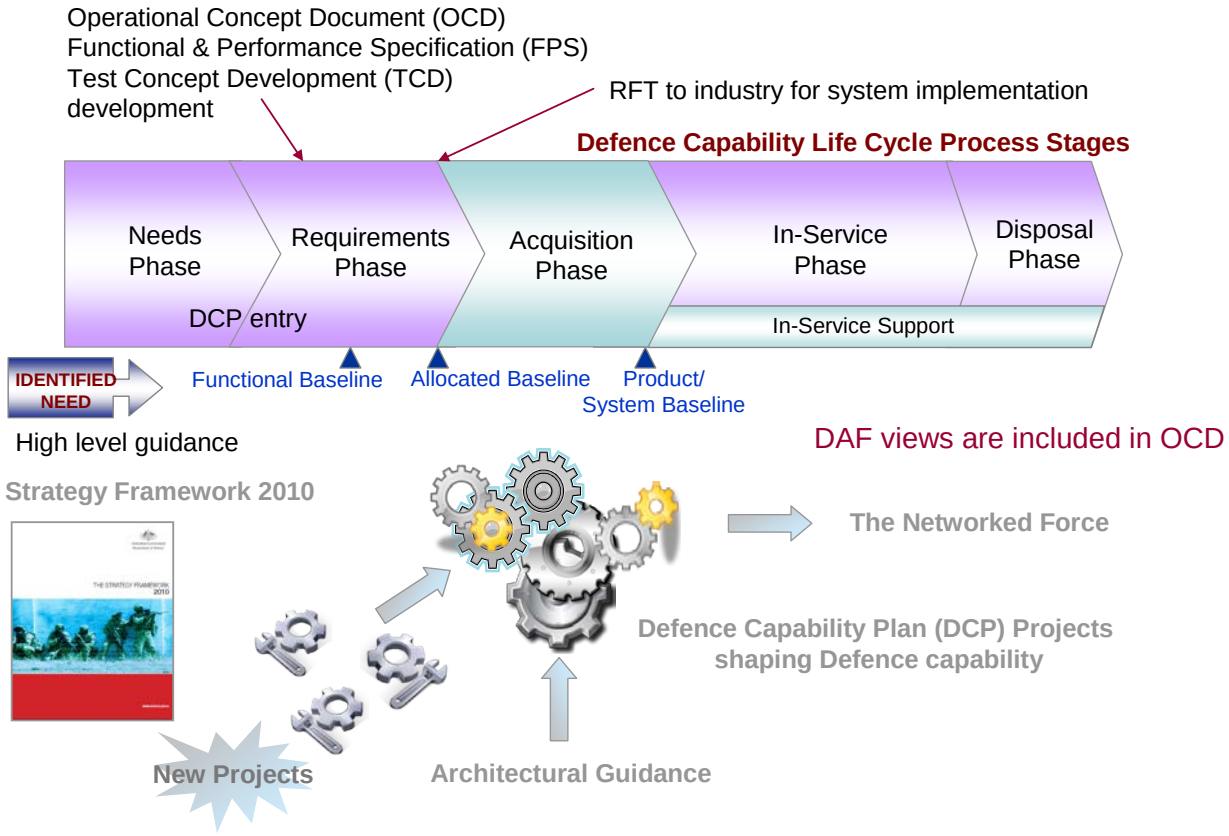


Figure 3 Defence Capability Development Life Cycle Process Mechanisms.

Capability development defines, gains Government approval for, and acquires capabilities that are employed by Defence in accordance with strategic priorities. Many organisational entities in Defence are required to actively participate in managing capability over its life cycle, as shown in Figure 4.

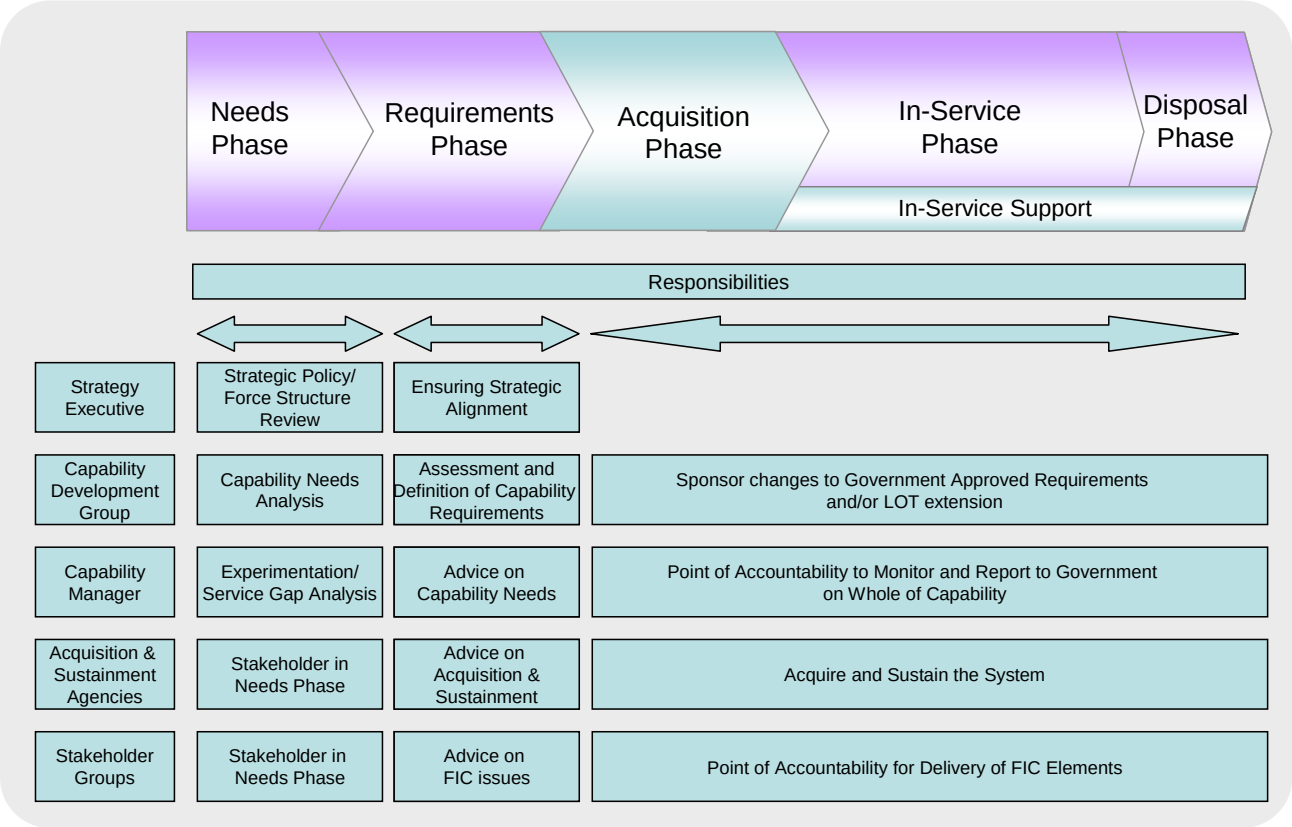


Figure 4 Notion of a Capability Life Cycle Showing Distributed Responsibilities (DCDH 2012).

Capability extends beyond the major capital equipment managed through the approval process by CDG and acquired by DMO. Capability is defined to encompass a set of Fundamental Inputs to Capability (FIC), which comprises:

1. Personnel
2. Organisation
3. Collective Training
4. Major Systems
5. Supplies
6. Facilities and Training Areas
7. Support and
8. Command and Management (DCDH 2012).

Higher level strategic guidance is promulgated through the FICs as shown in Figure 5.

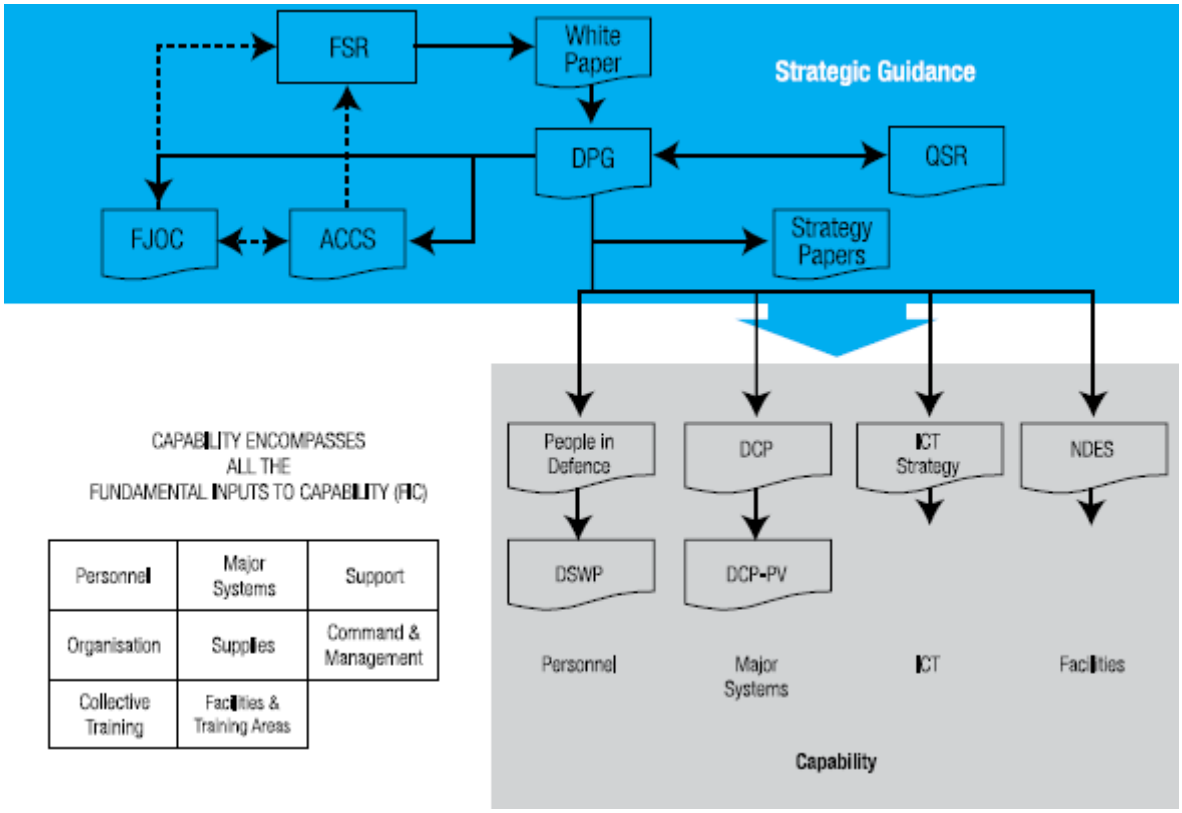


Figure 5 Promulgation of Strategic Guidance to the FICs (SF 2010).

Enterprise architecting is mandated for DCP projects with ICT implications. CDG's activity has primarily emanated from particular DCP Project activity as prescribed by the Defence capability development process (DCDH 2012). Capability Managers from the ADF Services have assigned responsibility for management of military related ICT capability.

3.3 White Paper Guidance on Future ADF Capability

Australian Defence policy is founded on the principal of self-reliance in the direct defence of Australia and protection of Australia's strategic interests. ADF capability is core to the defence of Australia. In the Defence context, capability is the capacity or ability to achieve an operational effect. An operational effect is described in terms of the nature of the effect and of how, when, where, and for how long it is produced.

In the 2009 White Paper, Defence was directed to develop a single integrated plan that embraced a "whole of enterprise" view, with clear linkages between strategy, priorities and resources, and with highly effective budget and resource management. Emphasis was placed on improving efficiencies without compromising effectiveness. It aimed to free up and reinvest resources, thereby reducing the pressure on increased Defence spending to offset the relatively small size

of the ADF and give them a war-winning advantage.

The ADF of 2030 is described as joint, integrated, and highly deployable. It is to be equipped with the capabilities and the people to take maximum advantage of technology to respond as Defence policy dictates. With regard to specific Defence information capabilities, the DWP 2009 refers to the importance of ISR capabilities, intelligence collection and assessment systems, space-based surveillance systems, cyber warfare, EW, strategic communications, battlespace management and command support systems to provide information superiority and deliver capability advantage. This is asserted to give the ADF a winning edge in comprehensive situation awareness, rapid decision-making, networked capabilities and the precise application of force (DWP 2009).

3.4 White Paper Guidance on Architecture-related Matters

The White Paper 2009 also provided specific guidance relating to situational awareness related capability where it directed that a major enhancement be undertaken of its ISR management processes and information architecture. It aspired to bring together all relevant assets into a Defence-wide architecture employing very secure, high capacity ICT systems, linking different systems employing universal data standards and protocols. This was to ensure critical information is available to those that need it in real time, eliminating stove-piping of information (DWP 2009).

3.5 White Paper Guidance on ICT Reform

The Government also directed remediation of Defence's critical "backbone infrastructure", including its ICT systems. To give effect to this remediation, Defence initiated a Strategic Reform Program (SRP) to address crucial deficiencies and capability gaps whilst producing significant efficiencies and cost savings to deliver genuine strategic national advantage (SRP 2010).

The White Paper 2009 expressed the need to draw together the various Defence information and communications domains into a single, properly governed information environment, delivering a capability fully aligned with the priorities set for the Chief of the Defence Force (CDF) and the Secretary (DWP 2009).

White Paper guidance sought to achieve business efficiencies and lower costs with more robust governance arrangements for Defence's ICT spending and the management of the Defence Information Environment (DIE) with a whole-of-Defence approach to ICT planning and decision-making. The proposed reforms were expected to deliver a secure and robust ICT capability to Defence that supports both war fighting as well as business requirements.

The White Paper 2009 also directed that a single Defence EA be adopted to support a more centralised and consolidated approach to delivering ICT services and infrastructure. This was to include consideration of scope, acquisition strategies, and delivery methodologies to provide a more targeted approach to ICT investment, reduce risks, and improve "time to market" for the delivery of new ICT capabilities (DWP 2009).

ICT reform in Defence was therefore being realised against the backdrop of the White Paper 2009, in particular, with regard to the Defence requirement for information superiority.

Alignment of higher-level strategic priorities with ICT related guidance is shown in Figure 6.

Figure 6 *Alignment of ICT Guidance with Higher Level Strategic Guidance (King 2010).*

3.6 Defence ICT Strategy Guidance

The notion of a single Defence EA implied a significant impending change to ICT planning and investment. Responding to higher-level Government ICT reform guidance and coinciding with the release of the 2009 White Paper, Defence also released a separate ICT strategy to drive ICT reform in Defence.

The *ICT Strategy 2009* acknowledged the close linkage between Defence's strategic objectives and the information and communications capabilities needed to achieve them. The ICT Strategy placed the remediation and reform of ICT capability provision within the broader context of the White Paper 2009 and the SRP.

The ICT Strategy sought to optimise ICT investment, closer stakeholder alignment, provision of agreed priority solutions, and strengthening of ICT capabilities as overarching strategic imperatives (ICTSTRAT 2009).

To provide visibility of Defence's ICT expenditure, all ICT funding decisions were combined within the context of a single Defence-wide ICT portfolio, underpinned by new procurement and approval processes and governance arrangements.

Supplementing White Paper guidance, the Chief Information Officer (CIO) was given responsibility for:

- developing Defence ICT policy, concepts and doctrine,
- developing a single Defence ICT architecture,
- establishing priorities and engagement strategies for ICT interoperability,
- coordination of ICT related FIC issues, and
- establishing the governance mechanisms to allow execution of the responsibilities and accountabilities.

The ICT portfolio comprised four sub-portfolios as follows:

- ***Infrastructure ICT Portfolio:*** ICT capabilities that affect all of Defence – encompassing common ICT assets such as data centre facilities, wide area networks, servers, workplace systems, storage, archival facilities, and systems that enable ICT operations,

- ***Intelligence ICT Portfolio:*** ICT capabilities that support intelligence outcomes,

- ***Military ICT Portfolio***: ICT capabilities that support Joint War fighter and Operations outcomes,

- ***Corporate ICT Portfolio***: ICT capabilities that support Defence business – including DSTO, DMO, Finance and HR systems.

This arrangement sought to better support stakeholder business priorities and facilitate more targeted direction of ICT resources, but within a Defence-wide governance purview.

3.7 Defence Strategy Guidance on the Single Information Environment

- The ICT Strategy called for the establishment of a Defence-wide ICT Operating Model and Enterprise Architecture to promote standardisation and consolidation of the DIE.

The DIE is depicted in doctrinal publication ADFP 6.0.2 as a reference model as shown in Figure 7.

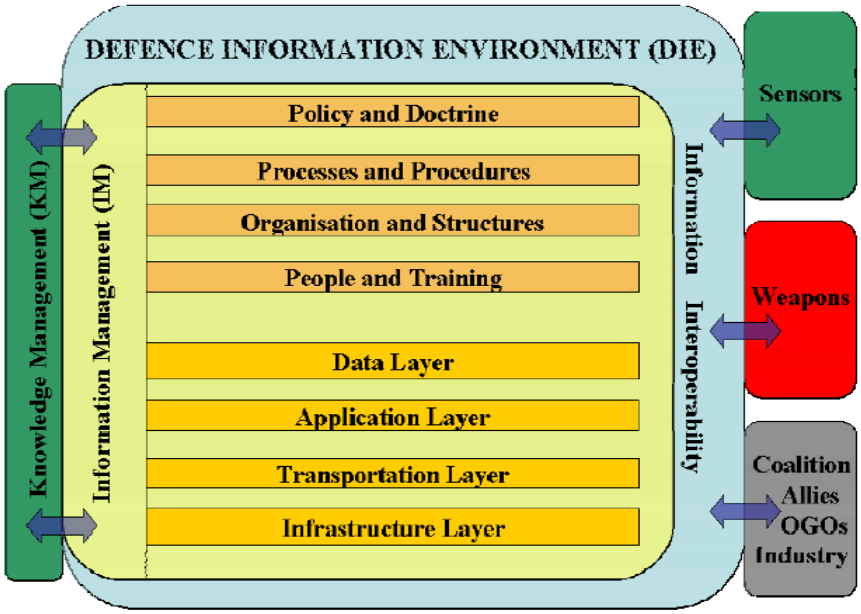


Figure 7 Defence Information Environment Reference Model (circa 2009) (ADFP 6.0.2 2009).

The SIE sought to integrate war functions and business functions so that technology could enable the information access and functionality needed to accomplish the Defence mission (ICSTRAT 2009).

The ICT Strategy identified the following objectives for the SIE:

- ICT scalability, flexibility and adaptability;
- Information speed and accuracy; and
- Technological capability edge.

The ICT infrastructure and process consolidation was encapsulated in a discussion paper published by CIOG in 2010 called *The Single Information Environment – Architectural Intent*. The Single Information Environment (SIE) was a key initiative within the SRP to realise the significant efficiencies and cost savings sought in Defence, and superseded the notion of the DIE (SIE 2010).

The scope of the SIE included:

- providing the communication needs for deployed military personnel;
- the secure transfer of information between the Australian Government and its allies;
- the connection of both people and military platforms to a single information environment; and
- provision of a standard ICT environment for corporate users in Defence.

Guiding principles for development, operation and management of the SIE included:

- Defence is aligned with the national approach to information management;

- Defence is provided with only one information environment for all of its organisations, occupations and security classifications;
- Information is managed; and
- The military is supported (ADDP 6.0 2012).

The SIE was envisioned as a single network connecting fixed and deployed locations, built on a single set of standards and products, encompassing all security levels. It is depicted in a reference model as shown in Figure 8.

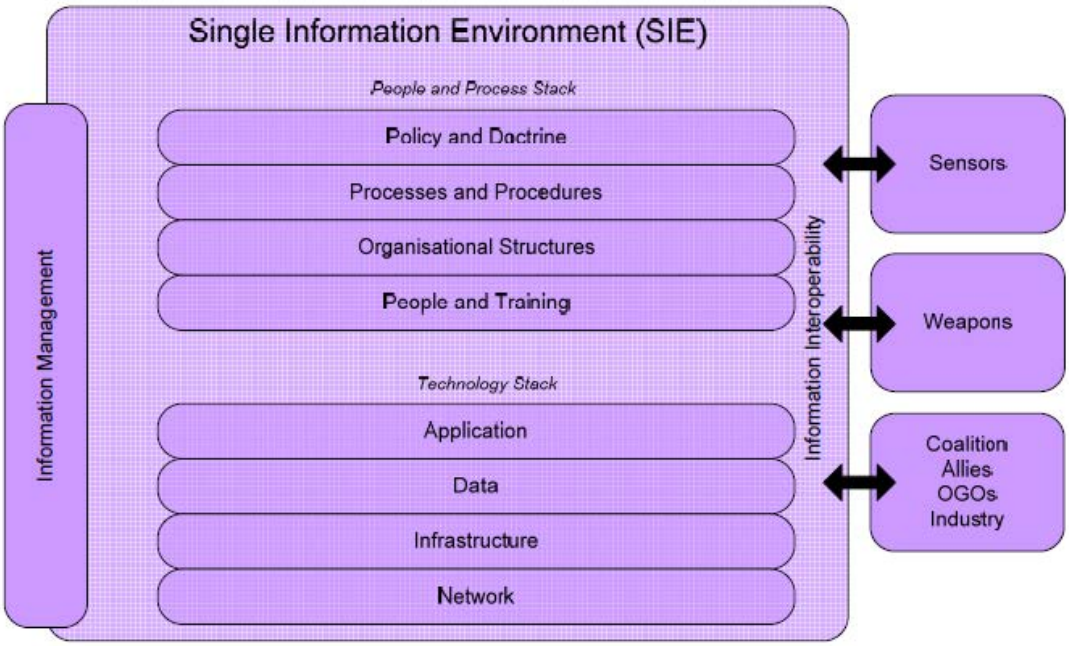


Figure 8 Single Information Environment Reference Model (ADFP 6.0.1 2012).

3.8 Defence Doctrinal Guidance and Policy Directives

Australian Defence Doctrinal Publications (ADDPs) and ADF Publications (ADFPs) are authorised joint doctrine for the guidance of ADF operations. Policy is prescriptive as represented by Defence Instructions, and has legal standing. Doctrine is not policy, and does not have legal standing, however it provides authoritative and proven guidance (ADFP 6.0 2012). The authority of the CDF to issue DIE-related policy and standard procedures is delegated to the CIO by Defence Instruction (General) (DI(G)) ADMIN 10-5 *Promulgation of Defence Information Management Policy Instructions*.

Communications and Information Systems (CIS) support has been accorded as central to the conduct of all functions in Defence. The concept of CIS support to operations recognises the intrinsic relationship between information in its broadest sense and combat power (ADFP 6.0.1 2012).

Although CIO no longer has coordinating capability manager responsibility for those projects that are largely ICT-related, the CIO would typically be appointed the Capability Manager (CM), with associated responsibilities spanning raise, train and sustain elements.

CIOG is also the Acquisition Agency for designated Defence ICT projects with prime responsibility during the Acquisition phase for the "major systems" FIC element. The CIO is also

the technical authority for architectures and standards required for all systems that interface with the SIE to receive and transfer data.

The CIO still has coordinating responsibilities for all of Defence's ICT. For military communications and information systems (CIS), this is exercised through the Strategic J6 (ADDP 6.0 2012). The Strategic J6 within CIOG has the charter to ensure that Defence has a dependable, secure and integrated information environment that supports Defence operations, ascribed as the DIE. The Strategic J6 is the sponsor for the ADFP 6.X *Communications and Information Systems Series* publication series.

The notion of the SIE has been incorporated into Defence doctrinal publications including the ADFP 6.0.X publications. While some doctrinal publications have been updated to reflect the notion of the SIE, other publications still refer to its predecessor, the DIE[6].

The instantiation of the SIE in the defence operating environment is described in doctrinal publication ADFP 6.0 – *Communications and Information Systems*. This publication presents the philosophical basis that is to be employed for the planning, capability development, acquisition, in-service management and use of communications and Information System (CIS) infrastructure by Defence, but specifically for the management and use of information by the ADF. ADFP 6.0 provides linkages between Defence's notion of the SIE, Defence capstone doctrine, other doctrine series, and subordinate Series 6 ADFP (ADFP 6.0 2012).

The SIE is described in ADFP 6.0 as the capability representing all aspects of information within Defence, including the information used within Defence, and the means by which it is created, managed, manipulated, stored, disseminated and protected. It encompasses the computing and communications infrastructure of Defence, the people, skills, documentation and management of systems that deliver that infrastructure.

ADFP 6.0 asserts that the SIE infrastructure is essential and integral to the continuity of central Defence functions and supports information domains as pervasive as:

- Command and Control;
- Intelligence, surveillance and Reconnaissance;
- Target Acquisition;
- Conduct of operations;
- Logistics;
- Strategic Policy;
- Capability development/management and resource management of:
    - Personnel
    - Finance
    - Asset Acquisition; and
- Through-life support / sustainment.

[6] Some pages on the CIOG website still use the DIE notation, for example, at URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/Defence%20Approved%20Software%20List.aspx with reference to the Defence Approved Software List (DASL), and at URL: http://ciogintranet/ICTServices/ICTHardware/Pages/ICT%20Hardware%20Policy%20.aspx with reference to Security Risk Management. The target ICT operating model within CIOG as of 28 September 2012 also refers to the DIE in the same context as prior to the launch of the SIE initiative.

The latest version of doctrinal publication ADDP 6.0 *Communications and Information Systems* ADDP 6.0 was released in 2012 to replace reference to the DIE with the SIE. Similarly, ADFP 6.0.1 *Communication and Information System Planning* was also updated in 2012 to reflect notions of the SIE. However, the most recent version of ADFP 6.0.2 – *Information Exchange* was released in 2009, and has not been updated yet to reflect the evolution of the DIE to the SIE.

3.9 Defence ICT Policy Directives

Strategic infrastructure management is facilitated by the CIO through the promulgation of Defence Information Infrastructure (DII) standards. The ATSL is the single authority for technical standards for the DIE/SIE[7].

The Defence Application Taxonomy (DAT) plays a key role in categorising Defence software applications within the DIE (IDATAX - no date)[8].

The DAT is co-managed in conjunction with other DIE/SIE standards and policy initiatives including:

1. Defence Architecture Framework (DAF);
2. Services Reference Model (SRM);
3. Technical Reference Model (TRM)
4. Defence Approved Software List (DASL)
5. Defence Standard Operating Environment (SOE)[9]; and
6. Defence/DSD Evaluated Products List (EPL).

In addition to the policies listed above, other policies dictating the management of information exchange within the DIE/SIE include:

1. **Security** – The Defence Security Manual (DSM)[10] describes security policy and procedures;
2. **Information Management** – ADDP 00.5 – *Information Management* provides the doctrinal reference for information management;
3. **Infrastructure Management** - The *Approved Technology Standards List* (ATSL) contains the mandatory technology standards that are to be used for all DII and CIS and management information systems (MIS) (ADFP 6.0.2 2009).

Notably, the CIOG website makes frequent reference to the DIE and the ATSL as well as the SIE and the DSMS. CIOG published EA guides and reference architecture books still refer to the DIE as depicted in Figure 7, while the NBA 2020+ Architecture Reference Book refers to the SIE as the target architecture for the Integrated Defence Architecture (IDA) (NBA 2020+ 2011). Pre-SIE and

[7] While the term ATSL is widely used across Defence, the hard copy has been superseded by an online version known as the Defence Standards Management System (DSMS). The DSMS can be accessed at the CIOG website at URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/Defence%20Standards%20Management%20System.aspx.

[8] The DAT, DASL, SRM and TRM can be accessed online at the CIOG website at URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/Defence%20Application%20Taxonomy.aspx.

[9] The current configuration of the SOE is designated as SOE 125.

[10] The DSM can be accessed online at the Defence Security Authority website at URL: http://intranet.defence.gov.au/dsa/dsm/

post-SIE terminology and concepts are therefore inter-mixed and used concurrently throughout the respective doctrinal and policy directives.

3.10 Government Guidance on ICT Reform

In response to the Gershon report (Gershon 2008), the Australian Government directed that ICT governance be strengthened at whole-of-government level, and that a series of ICT reform measures be embarked upon to improve the efficiency and effectiveness of the Government ICT marketplace. This provided additional impetus for ICT reform within the Department of Defence.

The Australian Government Information Management Office (AGIMO) was given responsibility to oversee the implementation of this directive. AGIMO's remit is to foster the efficient and effective use of ICT by providing advice, tools, information and services to help Australian government departments and agencies use ICT to improve administration and service delivery – referred to as e-government (AGIMO 2011)[11].

AGIMO developed the notion of an Australian Government Architecture Framework (AGAF) to assist in the delivery of more consistent and cohesive government services to the Australian community and to support the more cost-effective delivery of ICT services across Government.

The stated objectives of the framework were to:

- Provide a common language for agencies involved in the delivery of cross-agency services;
- Support the identification of duplicate, re-usable and share-able services;
- Provide a basis for the objective review of ICT investment by government; and
- Enable more cost-effective and timely delivery of ICT services through a repository of standards, principles and templates that assist in the design and delivery of ICT capability and, in turn, business services to citizens (AGA 2010).

In developing the AGAF, AGIMO adapted the Federal Enterprise Architecture Framework (FEAF) developed by the United States Government (FEAF 2007). The AGAF provided a similar set of highly detailed reference models as the FEAF to provide consistency in representation of the plethora of considerations regarded of common concern across multiple government agencies. (AGARM 2011).

A list of architectural principles was also provided to use as the basis for architectural decisions when designing cross-agency services and for assessing the underpinning processes and ICT system design (CASAP 2007). This was intended to facilitate service alignment according to business need rather than aligning to technology capability, supporting the consumer to efficiently carry out their business without unnecessarily adversely affecting their business processes. It assumed consultation with the consumer constituency and representation of constituency views in requirements definition and subsequent implementation.

Significantly, these services related to all cross-agency services and were not constrained to those only associated with ICT-related service delivery. Here, services are defined in the context of providing specific outcomes to service consumers with regard to the cost/benefit exchange

[11] A collation of whole-of-Government ICT Policy, Standards and Procurement Guidelines is provided on the AGIMO website at [online] URL: http://agimo.gov.au/policy-guides-procurement/.

and achieving value for money, spanning Government, citizens, businesses, community and other organisations (CASAP 2007).

Specific services are listed in the Service Reference Model (SRM) within the AGAF, and span diverse considerations from customer relationship management encompassing sales and marketing, brand management, and account management, to customer initiated assistance, work flow tracking, inbound and outbound correspondence management, business requirements management, business process change management, business hardware, software, and documentation configuration control.

In effect, the AGAF provides a governance framework for developing cohesive organisation-wide standard operating procedures across whole-of-government for common functions undertaken by different government agencies. It therefore provides the basis for decision making in ICT investment supporting those common functions, particularly in regard to commodity ICT. The Department of Defence is therefore subject to the same provisions in the AGAF as for other government agencies.

A more detailed description of the AGAF is provided in Appendix A of this report.

4. Background Influences – Enterprise Architecting

4.1 Notions of Enterprise Architecting

Numerous definitions and semantics associated with the terms *architecture* and *enterprise architecture* are used in Defence; these are inevitably context dependent.

At least three different interpretations are evident. It can:

1. represent the structures within an enterprise (extension of concept of an architecture of a system in systems engineering parlance);
2. be the description of an architecture of an enterprise (i.e. a suite of architecture artefacts or products);
3. be the business function responsible for producing the description of the architecture of the enterprise, and for deriving value from it.

The concept of architecture has been prominent in the fields of systems engineering and software engineering underpinning engineering development activity for several decades.

In the systems engineering context, the term *system architecture* has been associated with the mutually interdependent system concepts of:

- structure – what major elements are, how they are organised and decomposed, functionality, interfaces, and ties to system requirements;
- layout – physical arrangement, packaging and location of design aspects; and
- behaviour – system dynamics response to events to providing a basis for reasoning about the system (Maier & Rechtin 1997).

The term *architecture* and associated notions of *interface* and *integrated repository* have been enshrined in international systems and software engineering standards such as:

- ISO/IEC15288 : 2008
    - ***system architecture***
    - is comprised of subsystems, hardware components, software components and humans, and their interfaces (internal and external);
    - ***physical architecture***
    - is the hierarchical perception of system physical structure.

- IEEE Std. 1220-2005
    - ***design architecture***
        - an arrangement of design elements that provide the design solution for a product or life cycle process intended to satisfy the functional architecture and the requirements baseline.
    - ***functional architecture***
        - an arrangement of functions and their sub-functions and interfaces (internal and external) that defines the execution sequencing, conditions for control or data flow, and the performance requirements to satisfy the requirements baseline.

        - A functional requirement is a statement that identifies what a product or process must accomplish in order to produce required behaviour and/or results.
    - ***system architecture***
        - the composite of the design architectures for products and their life cycle processes.
    - ***interface specification***
        - the description of essential functional, performance and design requirements and constraints at a common boundary between two or more system elements.
    - ***integrated repository***
        - a repository for storing all information pertinent to the systems engineering process (SEP) including all data, schema, models, tools, technical management decisions, process analysis information, requirements changes, process and product metrics, and trade-offs.

- ISO/IEC/IEEE 1471: 2000
    - ***software architecture***
        - the fundamental organization of a system embodied in its components; their relationships to each other and the environment; and the principles governing its design and evolution (pertaining to software-based systems).

The ISO/IEC-1471 definition of software architecture has been adopted for use by both the US DoDAF and UK MODAF military EA frameworks, with particular emphasis on supporting ICT-related military capability acquisition activity (MODAF 2010), (DoDAF 2010).

Over the last two decades, the concept of architecture has been adopted by the business community, coined enterprise architecture (EA). It is primarily used to assist with business process re-engineering to facilitate better alignment of ICT investment with corporate strategy. In recent years, EA frameworks such as the Zachman Framework have extended the concept to apply more broadly to business practice in general. In this context, the enterprise is the organisation that is responsible for performing the various tasks within the purview of the business and investment re-alignment directive (Zachman 1987), (Zachman 2003).

In contrast to engineering practice, there is no commonly agreed definition of EA for ICT investment and business strategy management purposes; definitions vary between EA framework commercial vendors. There are no international standards or a preeminent EA-related body of knowledge. EA proponents can draw from other internationally recognised bodies of knowledge instead, including the Business Analysis Body of Knowledge (BABOK); the Systems Engineering Body of Knowledge (SEBoK 2012); the Software Engineering Body of Knowledge (SWEBOK 2004), and the Project Management Body of Knowledge (PMBOK 2009).

Again contrasting with engineering practice, there are no formalised notions of concepts such as system definition, system boundary, system component, and internal or external interfaces; nor notions of organisational, functional, or infrastructure hierarchy in EA frameworks such as Zachman, TOGAF, the US Government EA framework FEAF, and the Australian Government EA framework AGAF.

4.2 Enterprise Architecture Practice in Defence – Historical Perspective

The Defence capability development process operates in tandem with numerous other management, policy, regulatory and governance frameworks. Of particular significance, the

concept of EA was introduced into Defence, preceding the Gershon Report, the SRP and the Defence ICT Strategy by some ten years, to support MCE acquisition for particular Defence projects with a significant ICT component.

Along with other allied nations, Australia also embraced EA, first by Defence, then across broader Government. EA was introduced into the Australian Department of Defence circa 2003 under the auspices of the Defence Architecture Framework (DAF) [12],[13].

4.3 Defence Architecture Framework Guidance

The initial DAF concept was based on EA concepts developed by META Group[14] circa 2000.

The DAF essentially comprises a set of templates, containing specific diagrammatic forms and tables of prescribed information. These templates were derived from those originally developed by the US DoD under the auspices of the DoDAF (DoDAF 2010).

However, the DAF implementation differs significantly from the DoDAF. The US DoD approach provides significant guidance for the generation and management of DoDAF related information, and has sought to align architecture practice with their SE processes to assist in the system implementation, with strong emphasis on system and component identity, interface management, and information management (Okon 2012), (McDaniel 2012).

The Australian Defence approach is much simpler, comprising a mandate for inclusion of specific diagrammatic templates and tables in the OCD, one of the CDD documents required to be developed as part of the capability development process.

Instead of similarly following the DoDAF guidance, DAF guidance is provided in the form of a reference model to provide context to the DAF templates, as shown in Figure 9.

A tool set is also prescribed to prepare DAF artefacts. Guidance is provided on tool usage for artefact creation, where emphasis placed on use of templates to provide consistency of presentation of information rather than on coherency or management of information content. However, the method of collecting, analysing, managing and using the information is at the discretion of the respective projects. Tools include Microsoft desktop applications including Office Word™, EXCEL™, PowerPoint™, and Visio™; and IBM's enterprise architecting tool *System Architect*™.

Similar to commercial EA frameworks such as the Zachman Framework and TOGAF, the DAF is agnostic to engineering notions such as system boundary; system component, internal or external interfaces; nor organisational, functional, or infrastructure hierarchy.

[12] The initial version of the DAF is sometimes referred to as the AUSDAF.
[13] A detailed comparison between the DAF, DoDAF and MODAF frameworks is provided in (Hue 2014).
[14] META Group merged with Gartner in 2004. [online] URL: http://www.gartner.com/id=486650.

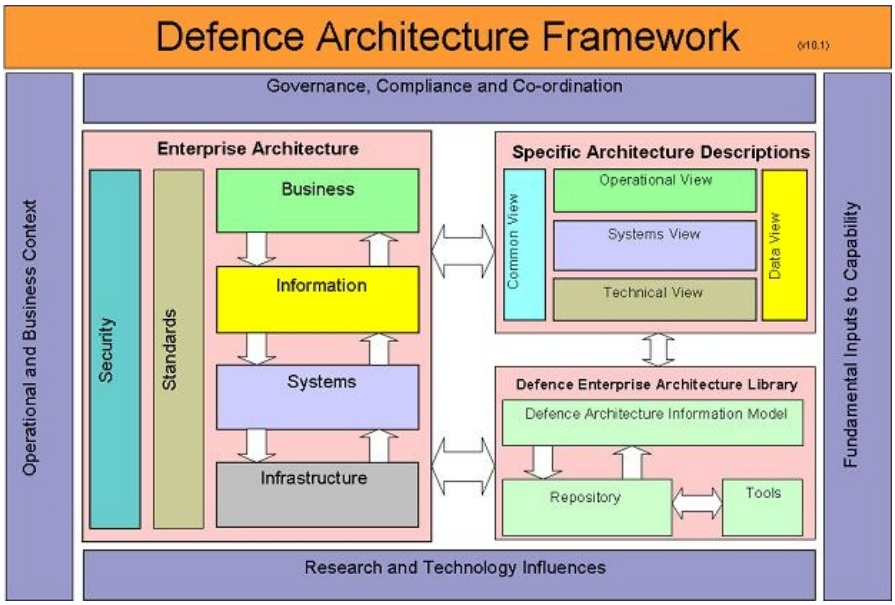


Figure 9. Defence Architecture Framework Reference Model (Purcell 2009).

The EA concept in Defence is still evolving, not only in response to AGIMO, White Paper and SRP initiatives, but also to changes in EA and systems engineering practice internationally, both in industry and military organisations.

Doctrinal publication refers to an evolved version of the DAF known as AUSDAF2. To reflect the intent of the period under examination, prior to aligning to DODAF 2.0, an earlier draft reference model for AUSDAF2 circa 2010 is shown in Figure 10.

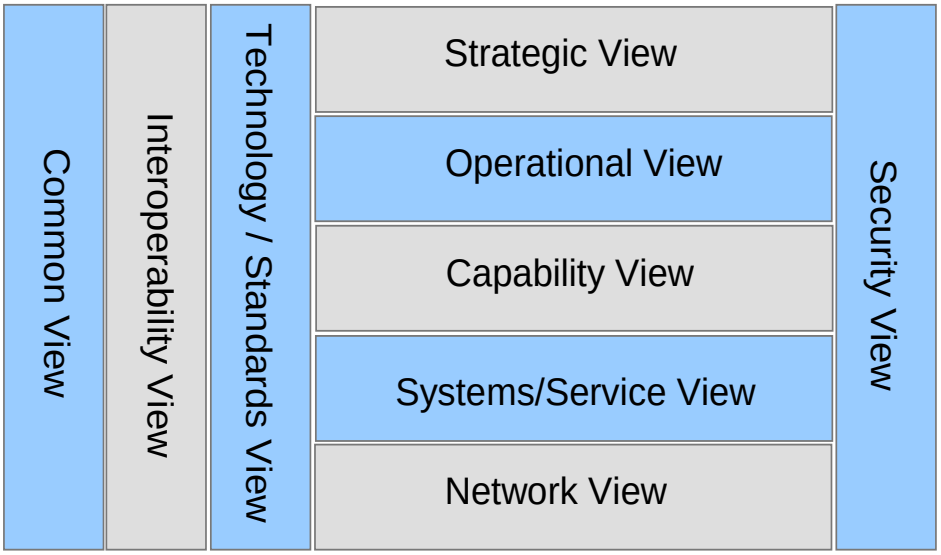


Figure 10 Draft AUSDAF 2 (King 2010).

4.4 Defence Doctrinal Enterprise Architecture Guidance

The Defence Enterprise Architecture (DEA) circa 2009 is described in doctrinal publication ADFP 6.0.2 as providing the framework to align Defence capability and outputs with strategic drivers.

Doctrinal publication ADFP 6.0.2 refers to the development of an enterprise architecture to provide efficient and effective use of information based on the premise that the organisation's business defines its information requirements. This in turn is used to determine what systems and infrastructure are required.

The DEA is depicted as a reference model within ADFP 6.0.2 as shown in Figure 11.

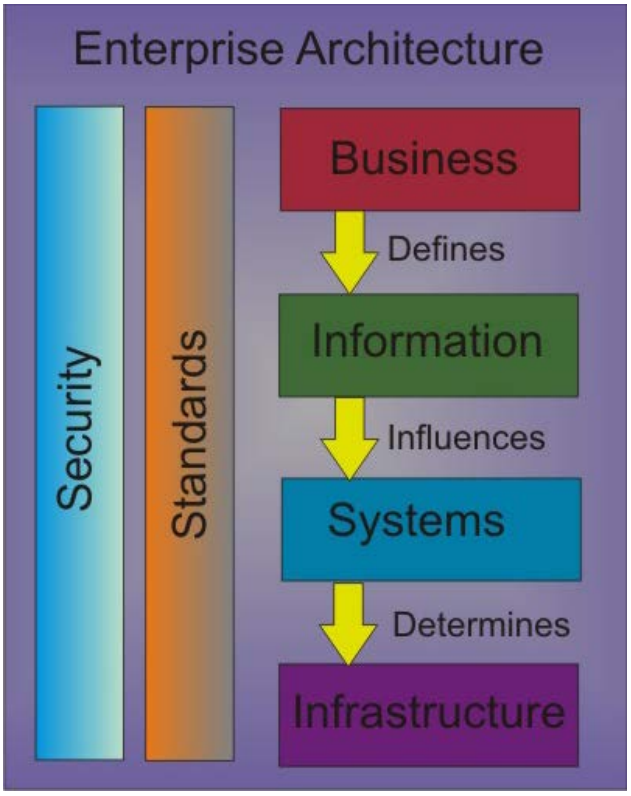


Figure 11 Defence Enterprise Architecture Reference Model (ADFP 6.0.2 2009).

The most recent version of ADDP 6.0 published in 2012 superseded the DEA, replaced with the notion of *The Integrated Defence Architecture (IDA)*. Both documents are current.

Notions of the DEA have been further promulgated within the Services where DI(N) ADMIN 43-2 describes the DEA as a federated model for EA, where each Group and Service within the Australian Defence Organisation (ADO) has been assigned responsibility by the Defence Committee for the development of their '*domain*' architectures as part of the overarching DEA. This process is governed by CIOG.

Navy, in turn, for example, responded by establishing the Navy Enterprise Architecture Framework (NEAF) to provide guidance on EA implementation across Navy. Guidance on

Navy EA implementation and products is provided in the Information Environment chapter of the Navy Business Procedures Manual[15]. Navy has coined the term Navy Information Environment (NIE) to identify Navy specific responsibility within the broader umbrella of the DIE.

Another example, DMO has established an enterprise architecture role within the DMO Business Information Systems. In contrast to Navy, DMO elected to focus on defining the architecture from a system and data perspective within the bounds of the DMO Information Management Strategy.[16] The existence of, and the type and form of relationships between the various DEA initiatives across Defence was not readily apparent.

4.5 Integrated Defence Architecture Guidance

As directed by the White Paper 2009 and companion Defence ICT Strategy 2009, a separate SRP initiative also commenced in 2009 within CIOG, to update the extant Defence Architecture Framework and to craft the skeleton of a new concept, known as the "*Integrated Defence Architecture*" (IDA). The intent was to provide an improved basis for funding decisions relating to Defence ICT-related infrastructure investment.

The latest version of ADDP 6.0 released in 2012 introduced the IDA as a means to align Defence capabilities and outputs with Defence strategic drivers. ADDP 6.0 asserts that enterprise architecting provides a common structure that can be used as a basis for capability planning and the development of consistent enterprise processes. This was intended to assist Defence to realise the maximum benefits from its ICT investments.

ADDP 6.0 describes the IDA as an enterprise architecture that addresses the relationships between all resources (including people, processes, ICT systems, other systems, information and operations) in Defence through providing principles and guidelines governing their design and evolution over time. The IDA was intended to enable the CIO to coordinate the development of SIE architectures and standard technical and procedural solutions (ADDP 6.0 2012).

The IDA is described in ADDP 6.0 as providing:

- a conceptual view of the future or target architecture for the Defence enterprise, represented as shown in Figure 12;
- a common medium for communication and planning between Defence business and ICT organisations;
- multiple perspectives of the Defence enterprise, including performance, business, systems/services, data, technology/infrastructure and security;
- relationships and dependencies –
    - horizontally (i.e. within a single perspective of the architecture)
        - what data is shared or self-contained;
    - vertically (i.e. across multiple perspectives of the architecture)
- what business functions and processes are supported by what systems/services; and
- key insights to enable strategic decisions and planning.

[15] Information on Navy's EA effort can be found on the Navy Intranet at URL: http://intranet.defence.gov.au/navyweb/sites/NBPM_IE/comweb.asp?page=35000&Title=Navy EA Framework.
[16] Information on DMO EA activity is provided on the DMO Intranet at URL: http://intranet.defence.gov.au/dmoweb/sites/IMR/ComWeb.asp?page=67956

ADDP 6.0 lists a number of architectural principles which are underpinned by legislative regulations that define the general rules and guidelines for the use and deployment of all resources and assets across the enterprise, including:

- **Principle 1 –** All Defence architecture will be referenced based, conform with, and take guidance from Defence strategic priorities and concepts of operation.
- **Principle 2 –** All architecture development will conform with and take guidance from the Australian Defence Architecture Framework 2 (AUSDAF2).
- **Principle 3** - Defence will have an IDA that has an enterprise focus and that provides enterprise-wide clarity and reasoning as well as supporting all Defence activities.
- **Principle 4** - Specific architecture descriptions should be iterative and provide for improvement, refinement and maturity against the mission and objectives.
- **Principle 5** - All architecture will conform to usability and reusability. They should address re-use as first option.
- **Principle 6** - All Defence architecture will deliver measurable results through endorsed standards and compliance processes.
- **Principle 7** - All architecture will be defined and documented in a common format and using a common language.

ADDP 6.0 also asserts that Service Oriented Architecture (SOA) is the preferred architectural style for the SIE, regardless of stakeholder operating environment.

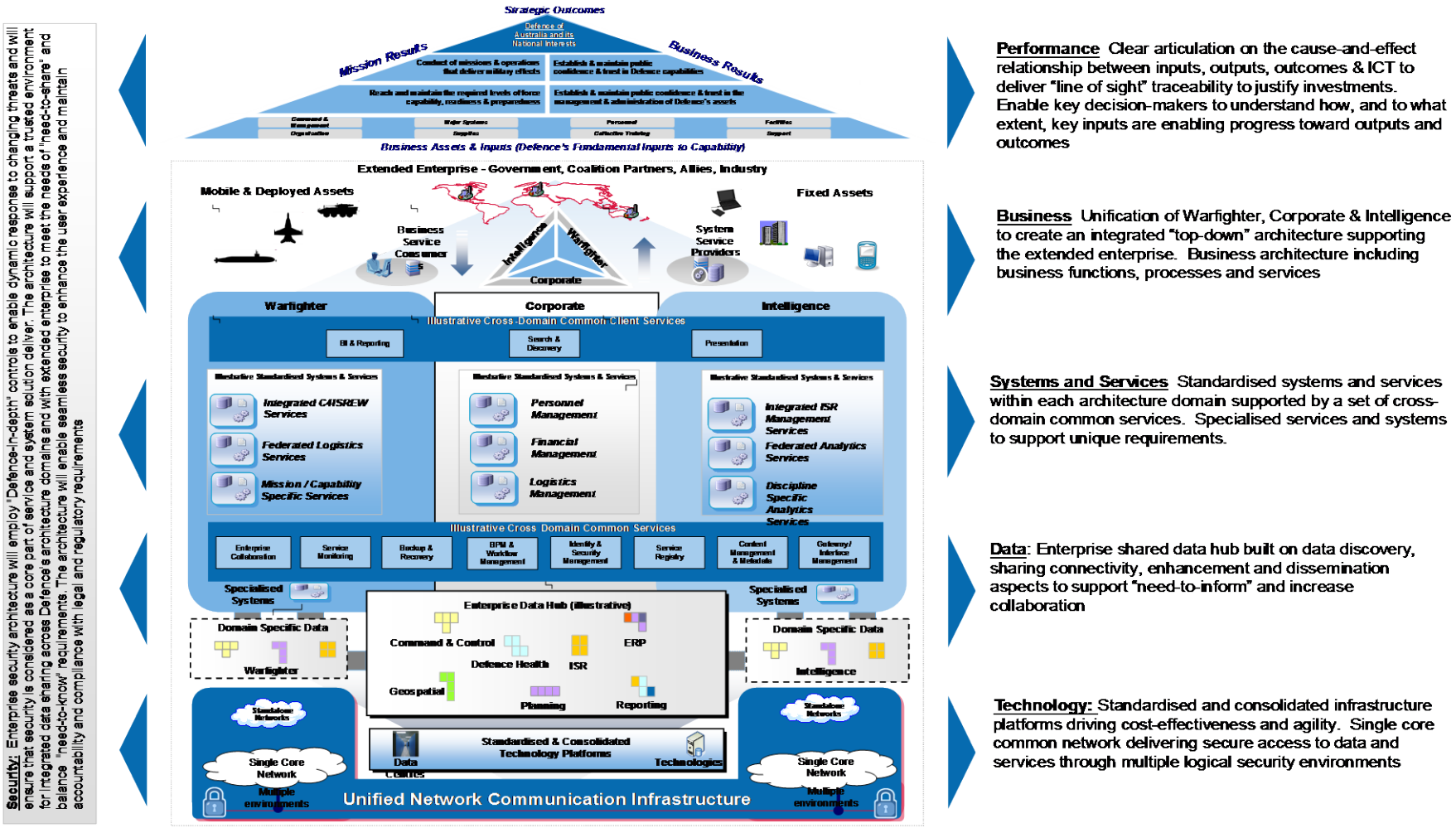


Figure 12 Integrated Defence Architecture Representation (ADDP 6.0 2012).

4.6 Further Enterprise Architecture Developments

Three key thrusts have emerged in latter Defence EA developments:

- one relating to artefact presentation,
- one relating to methodology, and
- one relating to reference models and reference architectures.

Contrary to the name of the initiative, the IDA was instigated as a federation of three separate EA sub-domains. CIOG's initial efforts were directed towards developing these distinct architecture sub-domains encompassing the warfighter, intelligence, and corporate business areas. The IDA is conceptually depicted as shown in Figure 13. The IDA is also represented as a reference model as shown in Figure 14.

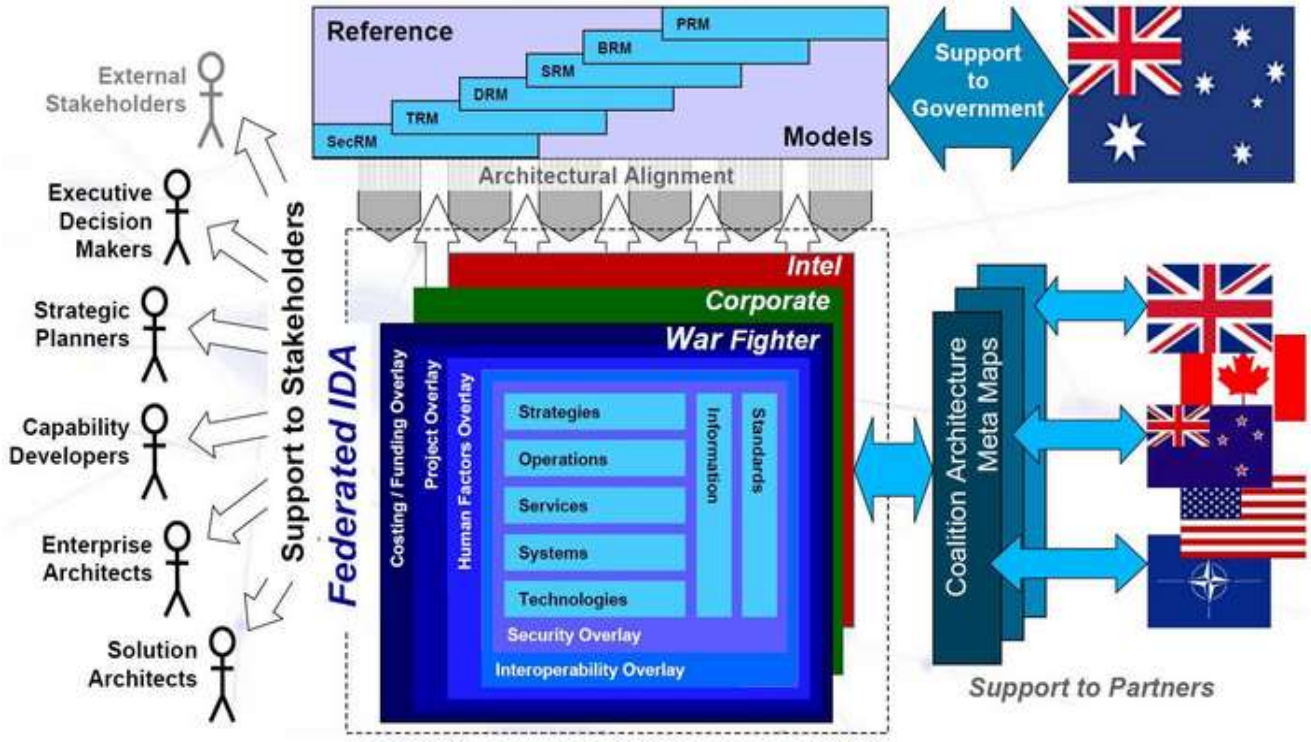


Figure 13 Conceptual Representation of the Integrated Defence Architecture[17].

[17] As described on the CIOG Intranet at URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/Defence%20Architecture%20Framework%20and%20Operating%20Model.aspx.

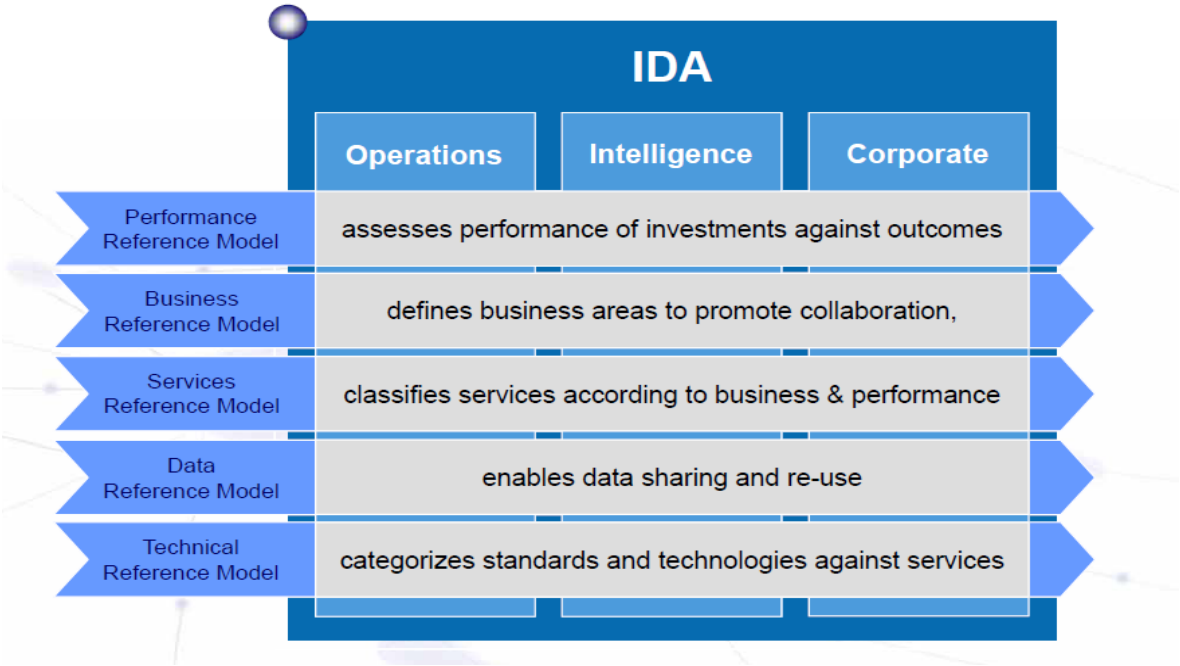


Figure 14 Integrated Defence Architecture Reference Mode (King 2010)

Initial IDA effort focussed on developing separate operating models for the three primary IDA sub-domains comprising:

- DCA – Defence Corporate Architecture (DCA 2011)
- JIA – Joint Intelligence Architecture (JIA 2010)
- NBA2020+ - Networked Battlespace Architecture 2020+ (also known as the Joint Operations Architecture (JOA) and Networked Battlespace Architecture (NBA)) (NBA 2020+2011).

These three IDA operating models corresponded to three of the four CIOG ICT sub-portfolios:

- Corporate ICT portfolio
- Intelligence ICT portfolio
- Military ICT portfolio.

Notably, there was no equivalent EA initiative corresponding to the fourth CIOG sub-portfolio, *Infrastructure ICT*, nor corresponding descriptive material. It was not apparent what criteria was applied to differentiate between ICT infrastructure in this particular sub-portfolio and the other three corresponding to the IDA sub-domains, nor why different treatment was afforded.

5. Review Context

5.1 Notions of Architecture Practice

The following background context is provided supporting the review of use of enterprise architectures in Defence.

Architecting, as described in ISO/IEC/IEEE-1471, is simply the activities of defining, documenting, maintaining, improving and certifying proper implementation of an architecture of a SW-intensive system. Thus, the data required to populate the artefacts can be extracted from analysis typically undertaken within a systems engineering or software engineering process; the artefacts providing specific viewpoints of the system and how it is used from an architecture framework perspective.

Detailed insight into the specific application of systems engineering and enterprise architecture concepts in Defence is provided in (Hue 2014).

5.2 Architecture Definition

The ISO/IEC/IEEE-1471 definition of architecture has been adopted for use in both the US DoDAF and UK MODAF military EA frameworks, and is referred to by Defence in the context of the DAF. The same definition has similarly been used within the JIA architecture reference book describing its contribution to the IDA.

The description of architecture offered in the NBA 2020+ and the DCA Architecture Reference Books differ from the JIA in that it describes EA as:

- the organising logic for process and infrastructure reflecting the integration and standardisation requirements of operating models (i.e. warfighter, intelligence and corporate) (DCA 2010), (NBA 2020+ 2011).

Stakeholders within Defence can therefore have markedly different semantics despite a common vocabulary, dependent on their particular professional discipline (e.g. engineering, IT, business analysis), prior specialist training undertaken, and current localised organisational context.

5.3 Architecture Descriptions

The DAF draws from the ISO/IEC/IEEE-1471 definition of an architectural description for SW-intensive systems. The architecture description is a collection of products (i.e. artefacts or populated templates) to document an architecture (DAF 2005a), (DAF 2005b).

The DAF does not explicitly acknowledge the existence of an actual system architecture itself, nor a specific methodology or analytical approach. Instead, attention is given to preparing artefacts drawing from a standardised set of scenario descriptions (i.e. use cases), re-cast from the perspective of the respective DCP Projects, with a focus on describing the applicable business (i.e. operational) processes.

In Defence, particular effort is taken to ensure the architecture descriptions remain conceptual in nature so as to support DCP project RFT preparation; conveying ideas rather than actual system implementations. They therefore remain largely solution independent. Consequently this limits their utility in performing system trade-studies and to drive real-world engineering

implementation (Hue 2014).

5.4 Enterprise Architecture Community of Interest

The EA Community of Interest (CoI) includes Defence and contractor personnel who:

- contribute significant resources to EA activity, and/or
- are significantly impacted by EA outcomes, and/or
- have specific EA process responsibility, and/or
- participate in EA activity in Defence, and / or
- contribute significant EA subject-matter-expertise (SME) and advice to EA activity, and / or
- contribute significant user domain subject-matter-expertise and advice to EA activity.

The EA CoI is therefore extensive and pervasive across whole-of-Defence, spanning organisations including:

- CDG
- DMO
- CM, including:
  - Army
  - Navy
  - Air Force
  - Joint – VCDF
- CIOG
- Defence Science Technology Organisation (DSTO)
- Other Defence organisations including but not limited to:
  - Defence Support Group (DSG); and
  - Intelligence organisations.

EA-related activity is undertaken from a variety of standpoints, depending upon the Defence organisation concerned:

- Strategy and Policy Division – Military capability gap analysis, provision of strategic guidance, force structure review, and concept development for new capability.
- CM – Force structure review and concept development of future capability for acquisition – operating environment perspective;
- Intelligence organisations – Concept development of future capability for acquisition – intelligence perspective;
- CDG - Concept development of future capability for acquisition – DCP Project perspective;
- DMO – Capability description for acquisition – DCP Project perspective;

- CDG, DMO - Capability Development Documentation (CDD) preparation (as described in the DCDH 2012);
- CIOG
  - EA and ICT policy custodians;
  - EA tool policy and license custodians;
  - EA training policy custodian and training provider;
  - DCP Project support – EA advice and ICT policy input;
  - Governance of DAF artefacts;
  - Corporate business process improvement;
  - IDA concept development;
  - ICT investment strategic reform ands rationalisation.
- DSTO - Operations Research (OR) in support of military capability gap analysis and capability definition activity;
- Intelligence Agencies
  - Provision of guidance for future capability acquisition pertaining to intelligence responsibilities; and
- Other organisations (e.g. DSG) – gap analysis and concept development for internal ICT support system upgrades – internal project perspective.

CDG effort is typically directed towards preparation of mandated EA artefacts to support DCP Project-specific CDD. This documentation forms part of the business case to obtain Government funding approval prior to issue of the respective Project RFT to Industry.

5.5 Enterprise Architecture Activity Purpose

From an IDA perspective, the stated goals of each of the IDA subdomains were as follows:

- DCA
  - The stated goal of the DCA was to provide a highly integrated logical structure that provided a whole of corporate description of the resources, objectives, capabilities and processes required to support the operational, supportive and organisational functions and services that the Corporate Business area provides to Defence. This goal was to be realised as a reference architecture for the corporate business domain (DCA 2010).
- JIA
  - The stated goal of the JIA was to enable agile, collaborative net-centric intelligence operations to support the decision making of Defence, by guiding both the implementation of the Defence Intelligence Network (DINet) concept and development of improved intelligence business processes (JIA 2010).
- NBA2020+
  - The stated goal of the NBA2020+ was to enable agile, collaborative net-centric

operations by providing an authoritative, unifying framework for Defence 'operations' for conducting Defence business in the warfighter space (NBA2020+ 2011).

The IDA subdomain architecture reference books asserted that the IDA subdomains would achieve their respective goals by capturing the key principles, processes, functions, rules, constraints and best practices relating to the conduct of the subdomain-related business.

The IDA architecture subdomains aimed to provide a conceptual description of a future target state that addresses the concerns of the respective subdomain stakeholders. This involved undertaking:

- To Be Analysis
- As Is Analysis
- Gap Analysis

where the outputs of the analyses were to be documented using DAF-style artefacts.

These analyses were expected to inform Defence intelligence stakeholders in terms of:

- How is business of the intelligence domain being conducted today?
- How will the business of the intelligence domain be conducted in the future?
- What the major changes must be implemented to achieve the desired change in the intelligence domain business?
- How well will the planned ICT capability support intelligence business in the future?
- What are the highest priority capability gaps in the intelligence domain that must be addressed (JIA 2010).

Expected benefits for the DCA and the NBA2020+ stated in the architecture reference books included:

- A 'fit-for-purpose' reference architecture for all subordinate architectures;
- Providing an operational reference architecture/design to guide component and project level architecture development;
- Increased awareness of the role of enterprise design to support strategic decision making;
- Implementation of architecture frameworks for developing integrated forces including the management and integration of legacy systems in a networked environment;
- Creation of a common understanding and shared awareness at the operational level;
- Increased support for efficacy for acquisition decisions;
- Increased support for interoperability within Defence, with Australian Government agencies and with domestic and international partners;
- Reduced duplication of Corporate capabilities; and
- Support for the implementation, where possible, of a service-oriented architecture strategy for systems development and design (DCA 2010), (NBA2020+2011).

5.6 Enterprise Architecture Activity Resourcing

At the time of the review, architecting effort in Defence was primarily undertaken by specialised

architects employed by CIOG, by contractors employed by CDG, DMO and CIOG, and by communications subject matter experts (SMEs) employed within the respective uniformed Services and Agencies.

CDG effort was typically supported by contractor personnel to prepare the CDD, including EA-specific material.

CIOG, in contrast, typically directed in-house development of corporate ICT (primarily COTS integration) infrastructure, supplemented by contractor personnel.

Resources for EA-specific activity were primarily sourced from:

- ICT Portfolio allocated resourcing
  - typically directed towards CIOG personnel
- DCP Project allocated resourcing
  - typically directed towards CDG, DMO, and contractor personnel
- Strategic Reform Program resourcing (pertaining to ICT reform)
  - typically directed towards CIOG and contractor personnel

Where dedicated EA resourcing was not provided (e.g. VCDF, CMs, DSTO), EA activity was resourced from the extant departmental operating budgets.

EA resources were typically allocated and managed on a project-by-project basis, with specific deliverables and timeframes.

5.7 Enterprise Architecture Practitioner Base

A core team of APS EA professionals in CIOG provided the nucleus of EA capability in Defence, supplemented by project-specific contractors, utilised by both CIOG and CDG. CIOG had responsibility for direction and governance of EA process activity. CIOG was also custodian of the EA material. For DCP projects with significant ICT content, an Enterprise Architect from CIOG was allocated to provide EA advice to members of the respective Project IPT.

User input (i.e. data/information/requirements) to EA activity was typically sourced from the respective Capability Managers (CM), spanning Army, Navy, Air Force, and VCDF, in line with extent Government policy, and framed in the context of the Defence Strategy Framework. User engagement typically took the form of one or more workshops (typically of less than 20 people), with invitations offered to specific user representatives. One-on-one consultation with specialist SMEs were also extensively used; SMEs were frequently asked to review EA artefacts prepared by CIOG and/or contracted personnel.

Contractors were typically engaged by CDG (mostly) and CIOG (in part) to prepare EA-specific material to include in the DCP Project-specific CDD, with particular reliance on CM supplied source data.

Some DSTO personnel and contractors engaged by DSTO prepared EA-specific material during the undertaking of Defence client-sponsored studies.

5.8 Enterprise Architecture Tools and Licensing

CIOG has custodianship of EA tools policy and management of corporate desktop computing tool licenses. CIOG have mandated the use of a prescribed tool set to support EA related

activity, comprising office and graphic drawing tools (Microsoft Office desktop computing tools PowerPoint™, Word™, EXCEL™ and Visio™), and specialist IBM EA tool, System Architect™.

Licenses for Microsoft Office tools PowerPoint™, Word™ and EXCEL™ are provided as standard software applications within the desktop computing "Common Operating Environment" (COE) in Defence. Visio™ is also a CIOG approved software application and can be purchased through CIOG, however, individual user licenses must be separately funded.

The Vitech Corporation systems engineering tool, CORE™, was also used both as a drawing tool and an analytical tool by some personnel, primarily DMO, DCP Project contractors and DSTO. In the past, DMO personnel with an established need (e.g. were members of a DCP Project IPT) had access to corporate licenses for both System Architect and CORE, however, other Defence personnel, including DSTO, were required to submit a separate business case for approval to purchase a license for CORE, and independently fund any additional licenses required.

Contractors funded their own tool licenses if their Defence client was unwilling or unable to provide a specific license (corporate or Defence client purchased) to them for the duration of the respective contract activity.

5.9 Enterprise Architecture Skill Base

The Defence EA skill-base was primarily home-grown, evolved in-house based on the principle of "learn by doing". Little or no specific recruitment activity was undertaken in Defence outside of CIOG to undertake EA-specific activity over the period of examination. Extant personnel were either redeployed and retrained, or their position descriptions adapted to add EA-related responsibilities. Contractors similarly accessed re-training opportunities to provide expanded support, and were heavily used by CDG in particular to support the preparation of DCP Project CDD.

EA activity in DMO and CDG was typically DCP project specific whereas EA activity in CIOG was ICT portfolio specific.; CM EA activity is typically focussed on their respective military operating domain (maritime, land, aerospace).

Many current CDG, DMO, VCDF, CM and contractor personnel were exposed to or involved in EA activity for an extended period of time preceding the launch of the ICT Strategy, and therefore had built up an extensive knowledge base based on pre-IDA EA practice.

The CIOG organisation has restructured several times since the initial launch of the DAF, but has maintained a specific organisational focus on EA activity. Extant personnel were re-trained with a business EA focus, bolstered by recruitment of several specialist commercial enterprise architects to expand the EA team in CIOG post-release of the ICT Strategy.

5.10 Integrated Defence Architecture Knowledge Base

Very little information is provided by CIOG specifically on the IDA itself, other than a brief description on the CIOG web-site, and in IDA subdomain-related documentation. Similarly, there is no reference on the CIOG Intranet to doctrinal publications such as ADDP 6.0 and ADFP 6.0.1, which have been rewritten to support the concept of the IDA.

Information on the IDA and its subdomains has been made available either in draft form or formally published by CIOG including:

- IDA BRM (IDA BRM 2011)

- JIA Reference Architecture Book (JIA 2010)
- DCA Reference Architecture Book (DCA 2011)
- NBA2020+ Reference Architecture Book (NBA2020+ 2011)
- BTIA Reference Architecture books and Project Guide (BTIA 2011a), (BTIA 2011b), (BTIA 2011c)
- CIOG Instruction No. 1/2001 – Service Oriented Architecture (SOA)
    - SOA Operational Concept Document
    - SOA Roadmap
    - SOA Governance Framework
    - SOA Reference Architecture
    - SOA Reference Model
    - SOA Business Model (SOA 2011)

Much of the above referenced EA documentation cannot readily be found on the DEFWEB or the CIOG Intranet when searched using the DEFWEB search engine. Copies of EA reference material can be obtained upon request from the CIOG listed points of contact.

EA artefacts prepared in support of CDD documentation are typically stored in the respective DCP information repositories. Since this information is not needed after securing Government funding approval, this information was typically archived and not subsequently updated. The archived DAF artefacts are therefore not particularly suited for re-use.

IDA related documentation differed from CDD documentation in that the information was purposely gathered and stored within a central location in CIOG by the IDA development team. Some information was stored on a specifically crafted Wikipedia portal, however, the completeness of the documentation set was uncertain, and referred documents were not necessarily up to date. It was not apparent how knowledge of the Wikipedia portal nor the IDA specific documentation existence was promulgated other than by word-of-mouth.

Other information was stored on the local Canberra server in project or activity specific folders within the top level "Common" directory. This meant Canberra based IDA team members had ready access to IDA specific information. Locally-based team members were able to readily share their respective source data and work output on the local work-area specific computer server. However, this information was not readily accessible or easily navigated over the Defence Restricted Network (DRN) for personnel geographically located outside the Canberra-based CIOG organisation (e.g. due to software application data sharing restrictions, license restrictions, network security access limitations, firewall restrictions, network connectivity limitations, poor wide-area network performance, and information management considerations).

Whilst the notion of an architecture repository was included as part of the DAF reference model at inception in 2003, aspirations to build a central repository of EA artefacts have been hindered by diffuse requirements and priorities. As of 2014, the Defence Architecture Repository System (DARS)[18] still has not been implemented.

[18] Several initiatives have attempted to implement Defence Architecture Repository System (DARS) based on the ASG Software Solutions *Rochade Metadata Repository*. Information on ASG-Rochade can be found at URL: http://www.asg.com/Products/View/ASG-Rochade.aspx.

It was therefore evident that corporate memory regarding EA activity and EA output resided in individual personnel engaged in the respective EA activity rather than in a formal knowledge repository. CDG personnel, primarily military personnel, had relatively short periods of involvement in EA activity compared with APS-based DMO, CIOG and DSTO personnel, due to the 2-3 year military posting cycle. Corporate memory, both in terms of tool usage and domain-specific information was therefore retained and accessible for much longer periods of time for civilian personnel and contractors compared with military personnel.

5.11 Enterprise Architecture and Defence Architecture Framework Training

When the DAF was first launched circa 2003, a specific training course was offered to Defence and contractor personnel at regular intervals of several months. This 2-day course primarily focussed on informing the trainee about the range of product types and templates within the DAF and how to populate the templates for use in CDD using Defence COE Desktop publishing tools such as Microsoft Office Word™, EXCEL™ and PowerPoint™. A 3-day course was also offered on Business Process Modelling and using the System Architect tool, distributed to trainees on a compact disk (CD).

In lieu of specific publications, information provided on the DAF primarily comprised of a list of architecture principles and a set of DAF templates, made available on the internal CIOG web-site[19].

When first mooted, A3 sized posters were published to provide an overview of the DAF (DAF 2005a), (DAF 2005b). Links to these documents are no longer provided on the CIOG web-site; instead relevant material is now provided as web-pages on the internal CIOG web-site.[20]

In the past, DAF familiarisation training was conducted by CIOG personnel using course material prepared in-house. Corporate consultants were also engaged on several occasions prior to 2009 to conduct seminars on particular EA methodologies such as the Zachman Framework. Training on tool use was typically provided by the tool vendor[21].

However, in recent times, with the advent of the IDA initiative, the availability of this training has receded, and has been replaced by self-paced online learning, offered through the Defence CAMPUS portal.

The CIOG EA website currently advises that the following EA training is available:

- Defence Architecture Framework (DAF) Campus Course (CRS-503);
- Business Process Modelling (BPM) Campus Course (CRS-895); and
- Architecture Tool Training
    - Bootstrap training for the tool 'System Architect' is currently provided in-house by the Directorate of Enterprise Architecture Practice (DEAP) in CIOG on a weekly basis.
- A 2-day course is also offered by the University of NSW at the ADFA Campus titled

[19] CIOG provided EA information can be accessed at the CIOG website at URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/default.aspx
[20] CIOG provided EA information can be accessed at the CIOG website at URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/default.aspx
[21] e.g. Vitech Corporation offer several training courses related to model-based systems engineering (MBSE) and on their "CORE" systems engineering tool. This can be accessed at URL: http://www.vitechcorp.com/services/training.shtml

'*Introduction to Enterprise Architecture*'.

Links are provided to U.S. DoDAF reference material on the CIOG web-site, which can be accessed at the discretion of the individual seeking the information. Extensive public reference material on the DoDAF and its application is readily available on U.S. web-sites; similarly for the MODAF in the UK[22] to support self-paced independent learning (DODAF 2010), (MODAF 2010).

Capability development documentation templates are provided on an internal CDG web-site[23], together with publication guides to provide guidance on populating the CDD templates. Capability process guidance and governance requirements are described in (DCDH 2012). No equivalent process or governance description is provided for DAF or other EA-related activity.

EA can also be studied externally at tertiary level, for example, Griffith University offer a Master of Enterprise Architecture, delivered by their School of Information and Communication Technology.

Courses are also offered by vendors associated with commercial EA frameworks such as TOGAF®, where OMG offers TOGAF® certification upon successful completion of their online course[24]. Access to these courses is at an individual's discretion. Although the recent IDA activity purports to utilise the commercial framework TOGAF®, it was not evident whether any Defence sponsored TOGAF® specific training was available.

5.12 Integrated Defence Architecture Training

No specific training or training material was provided to military or civilian personnel pertaining to the IDA developments other than that provided in the DCA, JIA and NBA2020+ architecture reference books. Instead, points of contact within CIOG were offered to enable one-on-one discussion between CIOG SME and the enquiring party.

CIOG initially assembled three stakeholder engagement teams, one for each of the IDA subdomains Military, Corporate and Intelligence. Each of these teams had an Enterprise Architect appointment (the SET-EA) who was responsible for liaising between the ICT Strategy and Architectures Branch (formerly known as Enterprise Architecture Branch) and other areas of Defence. The SET-EAs were the first point of contact for EA advice and requests for architectural support.

5.13 Enterprise Architecture Governance

DCP projects are subject to a prescriptive governance process as described in the DCDH 2012. CDD is prepared to support DCP Project business case submission to key decision bodies, the DCIC and the Defence Committee prior to seeking government approval for proceeding with the capability investment.

Governance requirements for capability investment have undergone significant change over the last several years. Prior to the Black Review in 2011, a separate decision body known as the

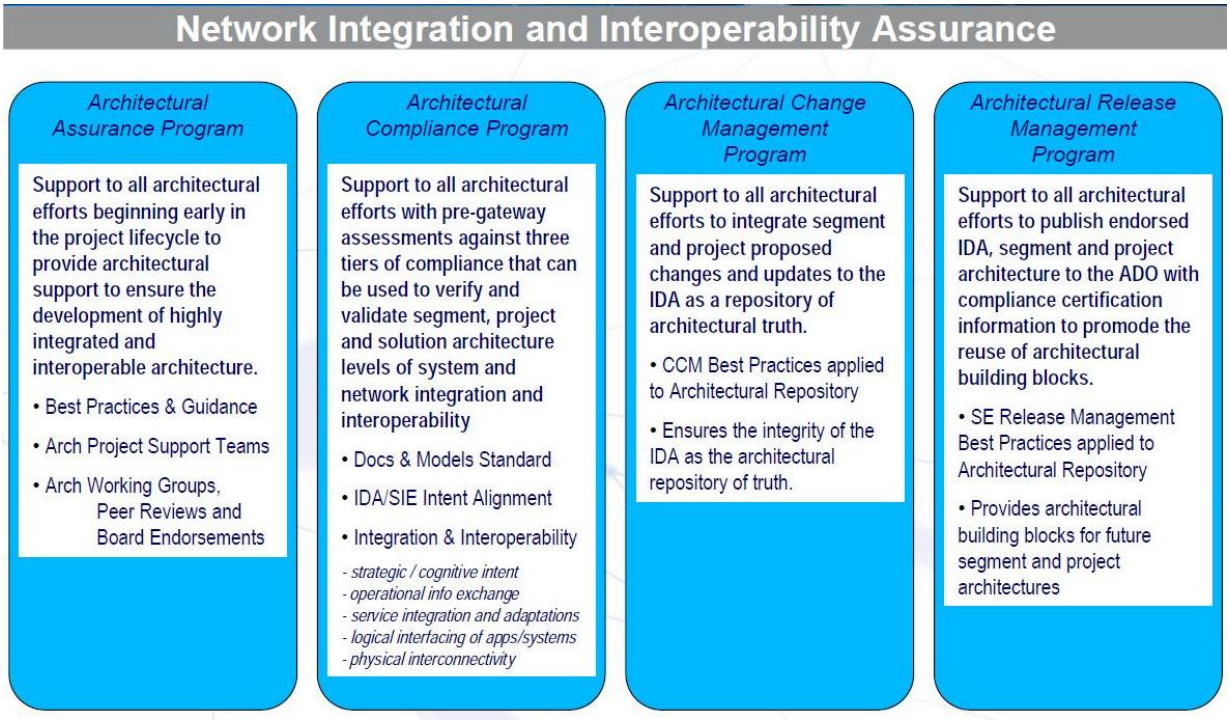
[22] Information on the DoDAF can be found online at URL: http://dodcio.defense.gov/dodaf20.aspx and on the MODAF at URL: https://www.gov.uk/mod-architecture-framework.
[23] Information can be found at CDG website URL: http://intranet.defence.gov.au/CDE/sites/ProcessMap/comweb.asp?Page=6935&menu=no.
[24] TOGAF® 9 certification training can be accessed at the OMG website at URL: https://togaf9-cert.opengroup.org/home-public.

Defence Enterprise Architecture Committee (DEAC) operated concurrently with the DCIC to provide specific oversight of ICT related investment. A separate Defence Enterprise Architecture Working Group (DEAWG) was established to provide a consultation forum for EA representatives from the different organisations across the entire Department of Defence. Initially, the DEAWG was given responsibility for review of briefing material prior to submission of ICT investment proposals to the DEAC. However, the DEAWG also ceased operation early in 2011.

Prior to 2011, those projects engaging in EA activity to support CDD preparation were also subject to an additional compliance regime known as the NCW Compliance Framework (Knight et. al. 2006). Architecture artefacts were reviewed by a NCW compliance specialist to ascertain the adequacy of the artefacts presented within the respective DCP project CDD to support the project business case. Since NCW compliance was mandated, any deficiencies in the DAF artefacts required remediation before approval could be accorded. This governance regime, only applicable to DCP projects with significant ICT investment, also ceased in 2011.

Subsequent to the Black Review in 2011, governance responsibilities for capital investment in Defence underwent significant change, affecting both DCP project approval and ICT investment approval (BLACK 2011). Responsibility for EA governance was given to CIOG with a mandate for all architecture development for the DIE to conform with and take guidance from the DAF and the IDA[25]. An Architecture Governance Framework was established as described in Figure 15.

This governance regime was made applicable to those projects delivering ICT capability within the purview of the IDA. Responsibility for IDA governance was accorded to the Directorate of Architecture Compliance within CIOG.



[25] The CIOG IDA governance framework and responsibilities are described on the CIOG Intranet at URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/EAB%20Responsibilities%20and%20Accountabilities.aspx and URL : http://ciogintranet/organisation/CTOD/ICTSAB/Pages/72906.aspx

Figure 15 CIOG IDA Governance Framework

Enterprise Architecture Branch (EAB) within CIOG was given IDA implementation responsibility with the following guidance:

- To build and deliver a robust Single Enterprise Architecture towards a common target architecture;
- To create a technical design authority and governance structure to guide and align all ICT within Defence; and
- To assist in the development of the target architecture by aligning planned and existing investments which will increase interoperability and reduce duplication.

Responsibility to meet IDA performance challenges was also assigned to EAB, to provide:

- linkages between major DCP programs and the target architecture;
- target architecture development to govern all Defence ICT projects;
- clarity on the target architecture vision;
- articulation of a 'top-down' business architecture to highlight the key business functions, processes and services across 3 stakeholder groups;
- identification of opportunities to reduce duplication and redundancy within Defence to reduce ongoing sustainment costs; and
- a target architecture that fosters and enables the re-use of assets.

The initial governance regime was then revised, instead, standing up an Architecture Review Board (ARB) in CIOG to undertake formal assessment for conformance with the DAF and the IDA. The Terms of Reference (TOR) for the ARB identified the ARB membership and arrangements for operation of the ARB, which included assigning responsibility to the ARB for undertaking the architectural design assurance activity on behalf of the DEAC. ARB responsibilities included conducting Architecture Compliance Reviews (ACR), approving architectural vision statements, and approving and monitoring of architectural contracts. Membership of the ARB was constrained to CIOG personnel. The governance regime described on the CIOG web-site, referring to the role of the DEAWG is obsolete. Scheduling of ARCs was notionally synchronised with designated DCP Project approval milestones[26].

An ARB was typically preceded by an Architecture Review Meeting (ARM), attended by various stakeholders. ARMs were instigated to facilitate oversight of the more technical aspects of EA in Defence, including providing feedback and guidance on project specific architectures. Generally a project would summarise the project's architectural intent and submit for peer review before proceeding to an ARB. ARM meetings were held on an ad-hoc basis, and were variously called by ARB permanent members, ARB invited members or the SET-EAs[27]. No dedicated funding

[26] Information on governance requirements including the ARB Terms of Reference can be found on the CIOG Intranet at URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/Architecture%20Review%20Board.aspx and URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/DAC%20-%20FAQ.aspx

[27] Information on ARBs and ARMs can be found on the CIOG Intranet at URL: http://ciogintranet/organisation/CTOD/ICTSAB/Pages/Architecture%20Review%20Meeting.aspx.

was provided to support reviewer attendance at ARMs or AWGs from organisations outside of CIOG. Attendance was self-funded.

In contrast to engineering best practice and capability development guidance, little specific guidance was provided on the conduct of the ARM, including considerations such as information to be provided, reviewer requirements, attendance quorum, project readiness criteria, project EA artefact review criteria or acceptability criteria.

Later in 2011, the concept of the ARM evolved to be replaced by Architecture Working Group meetings (AWGs). However, no TOR for the AWG was released, and no briefing information could be found which described the purpose, scope, review criteria, or reviewer criteria. The main difference apparent between the ARM and the AWGs called was the meeting invitation list, where AWG attendance was constrained largely to CIOG personnel and project specific personnel in lieu of the broader IDA stakeholder community.

Typically Integrated Project Teams (IPTs) and Project Manager Steering Group (PMSG) provided consultative forums for stakeholder engagement for DCP project activity. It was evident that ARM and AWGs pertaining to CIOG initiatives were significantly less formal that their DCP project counterparts, and attendance was far more constrained than the IDA stakeholder community.

Over the 2011 period, several ARMs and AWGs were held for a number of Defence internal ICT-based initiatives including eHealth, GEMS, Strat COP, BTIA, AUSDAF2 and SOA concept development. In some instances, such as the Strat COP project, the project utilised both an IPT and an AWG as consultative forums, although DCDH-style documentation was not made available to the AWG.

6. Review Findings

6.1 Enterprise Architecture Rationale

The rationale for engaging in EA activity, the EA experience, and perceived utility were found to vary significantly from one Defence organisation to another:

- CDG and DMO personnel were primarily engaged in EA activity to prepare DAF artefacts for inclusion in specific DCP Project CDD documentation as part of the respective DCP Project IPT effort.
  - There was no formal EA process prescribing the approach for preparation of the different artefacts.
  - Effort was confined to the minimum necessary to meet governance requirements for each DCP Project, which essentially comprised the specific artefacts mandated for inclusion in the OCD.

- CMs expressed pan-project interest, seeking to leverage specific DCP Project IPT activity to support development of future concepts of operation and delivery of ICT infrastructure in their respective operating environments to support future operations.

  - There was no formal CM EA process activity or template provided;

  - Type and scope of activity varied from one CM to another and from one Service to another, while they shared the common purpose of achieving a communications and information architecture that was capable of supporting future operations consistent with the guidance provided in the Strategy Framework.

  - It was evident that the CIOG focus on business process resulted in very little EA specific material being produced relating to ICT infrastructure, either extant or relating to the future ICT architecture being delivered by DCP projects and internal projects. This information was of particular relevance to CMs, and needed eliciting independent of the CIOG EA specific activity.

- CIOG interest varied according to ICT sub-portfolio responsibility and individual appointment:
  - Individual EA personnel could be assigned to specific DCP Project IPTs to offer advice on DAF artefact preparation and usage of CIOG mandated tools;
  - EA personnel engaged in DCA activity expressed interest in the business process modelling capability of certain EA tools to assist with business process re-alignment to improve business efficiency;
  - EA personnel engaged in JIA activity expressed interest in the ability to usefully describe a future intelligence information architecture;
  - EA personnel engaged in NBA2020+ activity expressed an intention to shape the future information architecture in the Joint Battlespace as a precursor to providing specific guidance to individual DCP Projects delivering military capability;

  - EA personnel engaged in IDA-specific activity expressed their future intention to shape EA practice and governance in support of developing the IDA. This also included:
    - Directing the composition of reviewers, and scope and frequency of reviews of EA related activity (i.e. determining governance requirements),
    - Directing the evolution of the DAF to next generation AUSDAF2,
    - Directing the evolution of the mandated EA tool suite, including management of corporate tool licenses,
    - Directing the nature and availability of EA-related training, and
    - Directing and managing the storage and availability of EA-related information.
  - It was not evident where CIOG personnel, involved in development and delivery of corporate ICT infrastructure, utilised EA concepts to assist the discharge of their responsibilities;
  - It was not evident where CIOG personnel, involved in the daily operation and management of corporate ICT infrastructure, similarly utilised EA concepts to discharge their responsibilities.
  - There was no formalised process guidance provided for CIOG EA activity.
  - Governance requirements for CIOG activity were ambiguous.
  - Risk management practices differed significantly between DCP Project capability acquisition and non-DCP Project ICT acquisition. Technically oriented risk management practices were not evident pertaining to ICT infrastructure acquisition.

- DSTO personnel expressed interest in two ways relating to the provision of scientific and technology advice to Defence clients including DCP Project IPTs:
  - EA tools could provide particular analytical capability of interest to support operations research studies.
  - DAF templates could form a useful method for presenting analytical outcomes during the undertaking of different operations research studies.
  - There was no formalised process guidance or governance required for DSTO EA activity other than normal DSTO policy requirements for peer review of work output prior to obtaining publication approval.

- Other Defence client groups, such DSG, expressed interest in the utility of business process analysis and standardised templates to assist in the expression and delivery of specific internal ICT infrastructure projects.

6.2 Integrated Defence Architecture Sub-domain Perspectives

A sampling of key stakeholders from across the EA CoI revealed the following perceptions relating to the IDA sub-domains:

- ***Corporate DCA Sub-domain***
  - CIOG personnel were predominant in EA activity pertaining to the DCA sub-domain.
  - Some CIOG personnel expressed satisfaction in the utility of business process modelling to examine the efficiency of extant corporate business processes.
  - CIOG initial infrastructure focus was on reducing the variety and increasing

standardisation of use of commodity desktop computing resources such as printers, printer and other ICT-related consumables, personal computers, and desktop application software, towards embracing the whole-of-Government ICT investment efficiency directives overseen by AGIMO.

- CIOG conducted at least one AWG meeting or ARM for several DCA related infrastructure projects including:
  - DeBI
  - eHealth
  - Strat Cop
  - GEM

- ***Intelligence JIA Sub-domain***
  - Intelligence agency personnel, supplemented by CIOG personnel, were predominant in EA activity pertaining to the JIA sub-domain.
  - The EA activity focussed on production of an architecture reference book to articulate future aspirations of the JIA target architecture.
  - Some CIOG personnel expressed satisfaction in the utility of the reference architecture book to provide a means to express the JIA target architecture.
  - The JIA CIOG effort was understood to have been separate from, and a relatively small effort compared with other independent activity in train shaping ICT-related intelligence capability.
- ***Warfighter NBA 2020+ Sub-domain***
  - CIOG EA activity was primarily focussed on developing:
    - A high level NBA 2020+ activity taxonomy;
    - the NBA 2020+ reference architecture book;
    - a high level BTIA activity taxonomy;
    - the BTIA reference architecture book.
      - Notably, the conceptual entity, BTIA, was not explicitly represented in the NBA2020+.
  - CM effort primarily involved provision of source data for inclusion in CDG CDD documentation and preparation of EA artefacts, review of EA artefacts and attendance at a BTIA ARM.
  - The largest EA effort was undertaken by CDG and DMO personnel, towards the production of EA artefacts for inclusion in CDD.
  - Additional CDG and DMO effort was afforded for review of NBA 2020+ EA-related materiel and attendance at a BTIA ARM.
  - Some CIOG personnel expressed satisfaction in the utility of business process modelling to represent the warfighting problem space, whilst acknowledging only a maximum around 80% accuracy in data was attainable at the time.
  - CDG, DMO and CM personnel expressed significant dissatisfaction in the combined utility of efforts to guide capability investment in the warfighter domain.

6.3 Stakeholder Concerns

The sampling of key stakeholders revealed a number of concerns relating to EA implementation. Expression of these concerns was consistent across different stakeholder groups across Defence:

1. None of the respondents from CDG, DMO, VCDF and the Services indicated they were getting value from the EA effort in Defence within the Warfighter IDA sub-domain.
2. None of these respondents indicated they were getting the answers they needed from the EA effort in Defence.

Concerns expressed by users included the perceptions expressed as follows:

- Architecting effort was not being directed to address user needs, limiting its utility, whereby it was reported by that:
  - Defence appointed enterprise architects did not sufficiently understand user problems;
  - The appointed architects lacked specific user domain knowledge;
  - The appointed architects had ineffective or inadequate consultation with users;
  - Architects did not sufficiently understand what their architecting output was going to be used for;
  - Architecture products were being produced to document decision outcomes rather than inform decisions, and therefore had limited or no utility to influence decision outcomes as intended;
  - Little output had been produced thus far which was seen to be useful, or which could demonstrate its potential usefulness.
- There was no formalised methodology provided for analysis and production of architectural information, leading to:
  - No guaranteed integrity of data;
  - No formalised information management practices for consistent storage and retrieval of EA-related information storage;
  - No consistency in architecting output and hence interpretation and use of architectural information;
  - No consistency in data models, terminology, and taxonomies across IDA Corporate, Intelligence and Warfighter architecture sub-domains to facilitate shared understanding, consistent application of guidance, and re-use of architectural information;
  - The capability acquisition process as described in the DCDH 2012 was not reflected in the architecting activity associated with the development of the IDA.
- There were significant issues with data validation and management limiting the usability and hence utility of architectural information, including:

  - no baseline data set had been established;
  - no single source of truth;
  - no ownership of individual data;
  - no change management;
  - no configuration management;
  - no data assurance;
  - no notion of data life cycle and data perishability;
  - no corporate architectural information repository;
  - no systematic method for data archival, retrieval and re-use;
  - no systematic method for identifying or imposing applicable mandates (e.g. technical standards);
  - no concept of design authority;
  - previous architectural information was not being maintained, and plans for future maintenance, including resourcing were not clear;
  - previous architectural information was not readily accessible, and it was difficult to ascertain apriori knowledge of its existence.

- There were significant issues with levels of stakeholder resourcing to support IDA architecting activity:
  - Architecting was perceived as requiring additional stakeholder effort, sometimes duplicating other effort, yielding little or no additional benefit because of limited utility in influencing decision outcomes and with limited re-use;
  - This additional stakeholder effort required was significantly under-resourced;
  - Lack of clarity of future funding availability was adversely impacting short term commitment where benefits might only be realisable in the longer term;
  - Using specific project funding to resource architecting effort for broader Defence application has purportedly introduced an inappropriate solutions bias for at least one DCP project, overriding acquisition decisions made previously through normal DCP governance processes.
- There were significant issues with governance, where the endorsement and review process for architectural information was not clear.
  - There were significant issues with the statement of intent as to how the IDA and accompanying architectural information were going to be governed, used, and maintained;
  - Governance mechanisms for architectural information were ad hoc, inconsistent, and lacking veracity;

  - The capability acquisition governance processes as described in the DCDH were not reflected in architecting activity. Governance associated with the development of the IDA did not take into account other capability acquisition considerations such acquisition strategies, acquisition constraints and project interdependencies;
  - The DEAC did not have Service Chief representation to provide oversight equivalent to the DC for those ICT projects with an impact on Defence Capability as defined in the DCDH[28];
  - NCW compliance mechanisms were dismantled without replacement of an equivalent Governance mechanism.

- There were significant issues with training of Defence personnel in architectures and retaining corporate memory.
  - There was a lack of training material and courses available to Defence personnel on architectures. Training had not been available on the DAF for an extended period of time (purportedly several years) (notwithstanding the provision of an online DAF course through Defence CAMPUS);
  - There was a significant skills shortage in Defence in architecture expertise;
  - Over-reliance on contractors significantly limited the ability of stakeholders to develop and maintain corporate memory.

6.4 Review Findings - Summary

The following summary of findings is provided.

Warfighter Sub-domain

1. There was widespread dissatisfaction expressed within the Warfighter Stakeholder community within VCDF, CDG, DMO and the CMs with the EA approach.
   - Stakeholders typically had a Defence capability development and acquisition focus with specific interests in information systems, communications and networking infrastructure topology and standards;
   - Stakeholders expressed interest in receiving improved capability implementation guidance to better manage capability and project interdependencies
   - Stakeholders generally had good familiarity with the DAF and the underlying EA principles promulgated by CIOG prior to the establishment of the IDA:
     - In particular, the focus on standardisation of architectural descriptions (i.e. EA artefacts).
   - Stakeholders generally did not believe they were getting value for the effort and resources being expended;
   - Stakeholders were generally not achieving their expected outcomes with the extant approach to EA;

[28] The DEAC was dissolved subsequent to changes in governance arrangements brought about after the release of the Black Review (Black 2011).

- Stakeholders were generally dissatisfied with the utility of EA effort, where it was not providing them with the guidance they were seeking;
- Stakeholders were generally not well-resourced to support the perceived demands to support the development of the IDA; and
- Stakeholders generally reported that their feedback was not achieving the desired impact.

Corporate Sub-domain

2. Some satisfaction was expressed within the Corporate sub-domain within CIOG with the extant approach to EA:
    - Stakeholders had lesser familiarity with the DAF and underlying principles promulgated by CIOG prior to the establishment of the IDA;
    - Some stakeholders were satisfied with the progress achieved thus far;
    - Stakeholders typically had a business process improvement focus to achieve Defence-wide SRP objectives, including greater efficiency and cost-effective delivery of corporate and ICT services;
    - There was insufficient enquiry during the review across the range of corporate services to establish a general level of satisfaction or dissatisfaction with the current approach to EA.

Intelligence Sub-domain

3. Some satisfaction was expressed within CIOG with the EA approach within the Intelligence sub-domain:
    - Stakeholders had lesser familiarity with the DAF and underlying principles promulgated by CIOG prior to the establishment of the IDA;
    - Some stakeholders were satisfied with the progress achieved;
    - Stakeholders typically had a focus on shaping future capability;
    - There was insufficient enquiry during the review across the range of intelligence services to establish a general level of satisfaction or dissatisfaction with the current approach to EA.

7. Review Insights

1. The investigations revealed widespread disparity about the meaning, applicability, purpose, methodology and resourcing of EA practice in Government and Defence. The basic EA principles being employed were unclear, despite reference to the TOGAF in some CIOG presentations. The definitions and explanations offered in CIOG EA-related publications did not accord with any of the referenced approaches including Zachman Framework, TOGAF, DoDAF, and MODAF, the PMBOK, SWEBOK, international systems and software engineering standards such as ISO/IEC 15288, ANSI/EIA 632 and IEEE 1220, nor the INCOSE published SEBoK.
2. It was evident that significant reliance was placed on individual points of contact within CIOG to provide guidance and advice on EA policy and IDA implementation. There was also significant reliance on specific Defence organisation intranets and common drives on local network servers to promulgate guidance and advice rather than promulgating in formally published documents. Much of this information was not subject to formal configuration control procedures. Where information was not dated nor tagged with documentation identifiers, it was difficult to determine what information was current and what was not, and what authority was being exercised. Significant guidance such as the SIE Architectural Intent 2010 was promulgated either as a discussion paper, or released as draft information, then adopted without updating. It was not evident whether/what feedback was sought or received, and subsequently promulgated as refined guidance. Information updates were not synchronised across the CIOG Intranet; policy, terminology and semantics were not consistent; and different DEFWEB and CIOG Intranet webpages and doctrinal publications did not necessarily reflect the most recent changes to CIOG organisation structure, governance responsibilities, policy and EA guidance.
3. Linkages between different organisational EA initiatives were not explicit so it was difficult to establish the existence of various policy initiatives; hence to determine the traceability and interdependencies between these initiatives, and to explicitly identify the applicable EA governance mechanisms in train across Defence.
4. It was evident that EA policy was not being uniformly applied by CIOG across all of Defence ICT. A significant effort had been underway since 2009, overseen by CIOG, to undertake ICT reform across whole-of-Defence. Initiatives included common sourcing and rationalisation of ICT support services, data centres, commercial-off-the-shelf software applications and desktop computing infrastructure (e.g. desktop computers, printers, and ICT consumables). It was evident a significant portion of this effort was taken place outside the auspices of the IDA and EA policy overseen by CIOG. It was not clear if or how the EA and non-EA based ICT rationalisation initiatives might relate to each other.
5. The centre-piece of CIOG's EA effort under the auspices of the DWP 2009 and the SRP was development of the notion of the IDA, supported by the evolution of the DAF to AUSDAF2, and the articulation of the notion of the SIE. However, there was no clear articulation of what the IDA was, the way to achieve it, nor its relationship to previous information capability strategy guidance provided under the auspices of the DIE.

   The IDA was described variously as:

   - A reference model;
   - A target architecture;
   - A federation of three IDA sub-domains, namely:

    - Corporate;
    - Intelligence; and
    - Warfighting;
- Single Enterprise Architecture;
- Defence Enterprise Architecture; and
- The Single Information Environment.

None of the above instantiations of the IDA correspond with notions of EA as described in the referenced commercial and military EA frameworks (e.g. the TOGAF, DoDAF, MODAF).

6. Similarly, while the SIE document was released as a discussion paper in 2010, no feedback was provided on discussion issues or outcomes nor whether the notion was formally ratified. The 2010 notion of the SIE was used as the basis for subsequent ICT investment planning and approval in CIOG without incorporating DCP ICT-based Project acquisition decisions.
7. It was evident that there was little consistency in application of EA principles across the various bodies of work undertaken under the auspices of the IDA. Three different EA approaches, with different interpretations as described in the respective sub-domain specific architecture reference books, were adopted for the three IDA sub-domains, DCA, JIA, and NBA 2020+.

   Furthermore, the architecting effort related to different timeframes which are not readily comparable:

   - The DCA presented a near term focus, emphasising business process remediation;
   - The NBA 2020+ presented a mid-term focus, emphasising the operational environment of 2020;
   - The JIA presented a longer term focus, emphasising the target intelligence capability sought.

   The JIA activity was undertaken concurrently, but decoupled from other effort to develop an Intelligence Surveillance and Reconnaissance (ISR) roadmap and target ISR architecture. The ISR architecture was not depicted within the IDA, despite manifesting within the same stakeholder operating domain. It was not clear how the two concepts related.

   Similarly, another initiative to articulate a coalition architecture was undertaken separate to, and independent of the DCA, NBA and JIA effort. The relationship between the coalition architecture was not depicted within the IDA, despite manifesting in the same stakeholder operating domain, so again, it was not clear how the two concepts related. No reference architecture book was prepared for this architecture.

   Another initiative to articulate the tactical battlespace information architecture (BTIA) was undertaken as part of the IDA initiative, however, it was not apparent how this related to the other operating domains. A dedicated reference architecture reference guide was developed for the BTIA. This information was not accessible from the DEFWEB or CIOG Intranet using standard web-site research requests.
8. It was evident that significant effort was expended towards documenting extant infrastructure and processes rather than providing guidance for future investment and process change. This baseline information was reported to be of little utility to DCP projects who were trying to depict an evolving but shared and cohesive view of future architecture states.

9. There was no reference to the notion of the IDA evolving over time. Despite reference to the ISO/IEC/IEEE-1471 definition of software architecture in DCA and JIA-related documentation, there was no specific articulation of the IDA concept and the EA principles and guidelines governing its evolution over time. Responsibility for this was devolved to the individual IDA architecture sub-domains.

10. No process mechanism was evident within the IDA initiative to identify applicability and promulgate specific guidance on mandated standards to achieve improved standardisation. A list of standards was provided within a CIOG administered document, *The Australian Technical Standards List (ATSL)*, however no guidance was provided on context of use, as to where these standards were already be in use, nor in what way and where they might be applicable in the future.

11. The applicability of EA policy directives and recommended EA practice for DCP projects was inconsistent with other capability development process and governance mandates, and with systems engineering precepts.

    The DCDH and international systems engineering standards refer to stakeholders spanning the entire spectrum of system development and evolution (those that use, own and acquire the systems, those that develop, describe and document the architectures, those that develop, deliver and maintain the systems, and those that oversee and evaluate systems development).

    Published IDA documentation refers to the Needs and Requirements Phases of the capability development process, but does not address subsequent stages of the capability life cycle. If EA concepts are not applied and managed consistently across the entire capability life cycle, and placed under configuration management, then it will not be possible to distil relevant EA information with good integrity after contract award. Availability of valid project-related information is integral to many of the analyses undertaken under the auspices of EA activity, including gap analysis, and capability and project interdependency analysis.

12. The notion of EA practice ostensibly applied to those enterprise-wide ICT infrastructure activities that span multiple ICT systems development. However, the IDA focus on business activities did not include consideration of enterprise-wide ICT infrastructure development. Guidance on ICT infrastructure acquisition and standards was provided in CIOG documentation outside the auspices of EA activity, such as lists of approved software products, approved standards and mandated desktop computer suppliers. These lists are available on the internal CIOG web-site.

13. No clarification was provided on how the notions of the IDA and SIE relate to other ICT strategic planning formalisms such as the notion of the DIE. The DIE provided the central focus for information capability acquisition and corporate ICT investment for many years. However, the SIE was agnostic to the DIE, and IDA briefing material was almost entirely agnostic of the SIE except for brief reference in the context of the ATSL. This brief reference inferred that the DIE related to communications and networking infrastructure, which was at odds with previous strategic guidance and the DIE reference model which included people, process and information within the scope of consideration. This information was not subsequently updated to reflect the changes effected by the 2009 ICT Strategy, SIE documentation nor IDA development.

14. Particularly for the warfighter domain, EA concepts were applied for specialised systems development that were inherently not enterprise-wide. However, the IDA approach lacked the formalisms and processes required to provide the necessary detail and rigour to manage implementation of specialised capability systems. The approach was largely agnostic to individual systems, components and interfaces; the system development life-cycle; delegated

authorities; and project management responsibilities (including risk management), all of which are fundamental to the implementation of architecture concepts.

15. Ostensibly, the IDA approach was developed based on the TOGAF v9 commercial EA framework. While solution architects from CIOG were appointed to provide EA methodological advice to assist different DCP project activity, they did not assume responsibility for architecting solutions as implied by TOGAF. Similarly, there were no representations of other key architecture concepts in TOGAF including the technology architecture. The technology architecture in particular is a key architectural concept in the TOGAF, providing guidance for future ICT infrastructure implementation. The IDA construct did not include the notion of a technology architecture, instead describing a technical reference model (TRM) (IDA TRM 2011). However the TRM was IT application-centric, and lacked sufficient formalisms and processes to provide the necessary breadth of technical detail and rigour required in lieu of systems engineering-oriented processes to drive specialised system implementations - neither for ICT infrastructure-related investment, nor for broader capability system implementation guidance and support.

16. Similarly, while implementation governance was featured in the TOGAF ADM, the EA governance and compliance regime stood up for IDA purposes was still evolving and lacking detail in implementation. Availability of briefing material to the EA stakeholder community was sporadic, and was heavily reliant on the CIOG Intranet for promulgation. It was not evident what criteria was used to establish sufficiency of:

    - consultation mechanisms,
    - stakeholder representation,
    - review of EA artefacts, and
    - reviewer subject matter expertise.

    In such circumstances, it was questionable whether EA-related information had suitable rigour to provide sufficient assurance to support key ICT investment decisions, or use by the broader IDA stakeholder community.

17. Finally, the IDA sub-domains DCA, JIA and NBA 2020+ were described respectively as business domains. NBA 2020+ guidance was premised on drawing an equivalency between warfighting and business. In the case of the TOGAF, the notion of business is understood to equate to commercial enterprise activity, delivering goods and services to a client base, either internal or external to the organisation. This is typically based on a balanced value exchange, under the auspices of an established governance process.

    Warfighting occurs in an entirely different value context to business activity; based on protection of sovereignty and national interests, in accordance with the Government imperatives of the day. The dynamics of the warfighting environment also differ markedly from a commercial environment. Warfighting activity, particularly at the tactical level, can be almost entirely unstructured, and the environment can be heterogeneous, hostile, and unpredictable. Therefore, flexibility, adaptability, and robustness are important attributes.

    This in stark contrast to highly structured business process activity occurring in a tightly controlled commercial operating environment, which may be in part, be amenable to ICT automation to enhance process efficacy, and ICT infrastructure standardisation to realise purchasing and operating efficiencies. From a capability development perspective, it was therefore misdirected to accord equivalency of warfighting to commercial business activity to drive capability acquisition as premised in NBA 2020+guidance (NBA 2020+ 2011).

8. Reconciling the Stakeholder's Perspective

When engaging in future EA activity, the following factors may be useful to consider from each stakeholder's perspective, to reconcile EA and capability development guidance and to establish a baseline for the expected utility of effort and outcome:

1. What issue is to be addressed?
2. Why does the issue need to be addressed?
3. Who is to address the issue?
4. How is the issue to be addressed?
5. What output is required?
6. What analysis is to be undertaken?
7. What input is required?
8. What scope is appropriate (e.g. FIC elements, operating environments)?
9. Who will be affected?
10. What are key drivers? (e.g. policy mandate, cost, strategic reform)
11. What are key influencing factors? (e.g. time-frame, environment, fidelity, security)
12. What assumptions are made?
13. What method of enquiry might be appropriate?
14. What attributes, characteristics or metrics are appropriate?
15. What methodologies and tools might be useful?
16. What format is appropriate?
17. What are the internal constraints?
18. What are the external limitations?
19. What skill sets are required?
20. Where should the respective skill sets be applied?
21. What training is required?
22. What output might be relevant to store in a specific repository for later re-use?
    - Use by whom, in what format, and for what purpose?
    - What context?
    - What attributes?
    - What assumptions?
    - Where is this information to be held?
    - How is this to be made known and accessible?
    - How is this information to be managed and who by?
    - How does this information relate to other Defence information repositories?

9. Conclusion and Recommendations

EA, as described in commercial EA frameworks such as TOGAF, has been specifically crafted to analyse shortcomings in corporate business practices. This is undertaken with a view to improve process efficacy through the organisation-wide adoption of commodity ICT technology and COTs SW applications with no or little adaptation. This aligns well with Strategic Reform Program imperatives.

A harmonised whole-of-Defence architectural approach may well facilitate significant process efficiency gains and reduced cost of commodity ICT investment. However, it was evident that there are numerous problems with the enterprise architectural approach, which was attempting to develop a uniform ICT environment spanning whole-of-Defence, but against the backdrop of multiple and overlapping governance frameworks, conflicting requirements, and disparate priorities.

The study revealed widespread disparity about the meaning, application, purpose and methodology of EA practice in Defence. Guidance on EA practice in Defence was fragmented, and was significantly reliant on cross-referencing to disparate third party references.

The study also revealed significant stakeholder dissatisfaction with the utility of the EA activity output in shaping individual stakeholder capability acquisition decisions.

Competing priorities in different organisations within Defence can render EA practice ineffective and divergent from individual organisational imperatives. This view was particularly prominent in those organisations identifying themselves as stakeholders within the warfighter community, including CDG, DMO and the CMs. Stakeholders in these organisations expressed significant dissatisfaction with the utility and value of EA practice as manifested within the IDA initiatives and preparation of DAF artefacts in support of CDD documentation.

Warfighter stakeholders, in particular some CMs, expressed their concern about the impost of supporting numerous EA activities, including repeated requests for provision of source data and review of EA output, without provision of commensurate resources, and without discernable benefit to the stakeholder.

It was also evident that the EA approach promulgated in Defence was not meeting many warfighter stakeholder needs; it was not providing the relevant advice needed to support the respective organisations' differing roles and responsibilities.

By its very nature, the warfighting environment is complex, heterogeneous, and volatile. It involves interaction with many different parties with very differing needs. Defence EA practice examined lacked the formalisms to take into account the implications of local factors such as the threat environment and the physical environment.

The imposition of large-scale, standardised corporate solutions in the warfighting environment without consideration of the suitability and limitations within the specific threat environment and physical environment context is ill-advised.

CIOG EA practitioners sought to broaden the application of EA concepts beyond ICT to the capability development and acquisition process to address questions that are inherently non-ICT in nature, and non-enterprise-wide. However, Defence EA practice is agnostic to a number of key technical and management processes associated with the capability development process and industry engineering best practice, to help account for the inherent complexity of the operating environment, including principles of requirements management, risk management, quality assurance and life-cycle management.

EA practice examined does not provide sufficient robustness to replace the long-established systems and SW engineering practices for modification or development of new, more complex ICT implementations, for example, necessitating use of customised or distributed networked SW applications, or non-commodity ICT infrastructure. The outcome of any such approach would be skewed accordingly, and likely to suffer significant integration problems due to the presence of potentially numerous latent defects.

Similarly, the EA approach described is not suited to address problems that are inherently non-enterprise wide in nature, and are not suited to drive investment decisions in capability which have additional non-ICT specific considerations. As such, EA practitioners without commensurate systems or software engineering expertise would be ill-equipped to scope the problem space in the appropriate context and apply the requisite skills to achieve the efficiency and efficacy outcomes.

The following recommendations are offered:

1. To clarify and explicitly articulate from a whole-of-Defence perspective:
   - What are the meaning, scope, applicability, intent and limitations of Defence EA practice?
   - How do the respective EA initiatives fit together?
   - What are the implications of whole-of-government EA guidance and how are these to be reconciled in the Defence context?
   - What assumptions are being made?
   - How should EA practice be implemented, in terms of methodologies, technical and management processes, and governance?
   - How does EA relate to other Defence technical and management processes?
   - How should EA practice be promulgated?
   - Who should be involved and in what way, in terms of roles, responsibilities, contributions, end-usage and beneficiaries?
   - What stakeholder authorities have precedence?
   - How is EA practice beneficial to the stakeholder community?

2. To clarify and explicitly articulate how the IDA and its accompanying EA effort can provide utility in support of the capability development process over the entire capability life cycle.

3. To establish and manage an accessible and readily navigable information repository encompassing:
   - the relevant architectural methodology:
   - assumptions and constraints;
   - dictionary of terms;
   - architecture description language;
   - architectural information (pertaining both to specific projects and higher level IDA guidance);
   - artefacts;
   - guidance for tool set up and usage; and
   - information management guidance.

4. To enhance the stakeholder consultation process to ensure appropriate feedback is obtained and followed through to the satisfaction of the parties concerned.

5. To enhance governance mechanisms to:
   - assure the integrity of architectural information and its suitability for the intended usage;
   - the appropriate guidance is provided to stakeholders; and
   - appropriate authorities are enforced.

6. To develop an appropriately skilled workforce, with ready access to suitable training courses, training material, and tools, which reflect the specific intent and usage in the Australian Defence context.

7. To implement an evaluation process that monitors and reports on the progress of reforms to facilitate improved utility of EA effort.

Further enquiry is also recommended to:

- Examine the range and nature of architectural information being generated across Defence to identify criteria to discern which information is architecturally significant from a whole-of-Defence perspective.
  - for example, distilling those systems or components, characteristics, and/or relationships that have broader organisational impact and therefore may be candidates for further standardisation on a larger scale.
- Examine possible Measures of Performance (MoP) and Measures of Effectiveness for the significant architectural elements, and possible methods for performance monitoring.
- Examine the potential of OR and systems engineering methodologies to undertake analyses to support the EA outcomes sought to value-add to other forms of enquiry.
- Examine methods for more effective promulgation and governance of EA-related matters to the broader stakeholder community.

10. List of Consultations

The following personnel were consulted during the conduct of this review of architecture use in Defence.

Position	Appointment
CIOG	
A/Director General Enterprise Architecture (DGEA)	Mr. Graham King
Director Enterprise Architecture (DEA)	Ms. Gina Kingston
Director Governance Regulation Assurance and Compliance (DRAC)	Ms. Jennifer Murray
Enterprise Architect CORPORATE SET (EAC)	Mr. James Wood
A/Director Architecture Practice Management (DAPM)	Mr. Ric Allen
Director Applications Architecture	Mr. Iain Johnstone
Enterprise Architect INTEL SET (EAI)	Mr. Peter Kalkman
Technical Director - Corporate	Ms. Shuping Ran
Deputy Director Business Architecture (DDBA)	Ms. Catherine Palmer
Executive Director – Enterprise Business Architecture and Information Management	Ms. Vanessa Horton
RPDE Task 38 Strategic COP Project	Dr. Ron Meegoda
DMO	
Director of Systems Engineering, Materiel Engineering	Dr. Shari Soutberg
DMO Support, DMO Standardisation Office	Mr. Dave Gapp
Director JP 2089, Tactical Information Exchange Integration Office (TIEIO)	Mr. Kevin Pottinger
Director Emerging Projects, DMO. Formerly Enterprise Architect – MILITARY SET (MILSET-EA), CIOG	Mr. Paul Pappas
Director ADF Tactical Data Link Authority	Mr. Dennis Healy
TIEIO	Mr. Jim Denton
TIEIO	Mr. James Meredith
Director Logistics Information System Management	Mr. Selby Dyer
CDG /CM	
Deputy Director Maritime Communications, CDG	CMDR Jeff Milward
Deputy Director Land Communications	LTCOL Steve Welsh
RAN TIED Capability Coordination Manager	CMDR Michael Reis
Deputy Director Battlespace Integration – Network Centric Warfare (DDBI-NCW), VCDF	CMDR Murray Smith
Deputy Director Battlespace Integration Performance Management, VCDF	LTCOL James Van Heel
Deputy Director Battlespace Integration ICT	Mr. Mark Saunders

(DD-BIICT), VCDF	
Director NCW-Army, AHQ	COL Shaun Love
Deputy Director Land Communications, CDG	LTCOL Steven Welsh
Staff Officer 1 CISEW, AHQ	LTCOL Greg Novak
Deputy Director ICT – Army (DDICT-A);	Mr. Ray Spoor
Director Network Enabled Warfare – Army (DNEW-A)	
Director Navy Command Control Communications and Computing (DNC4)	CMDR Matt Doornbos
Deputy Director CIS Capability Planning, AFHQ	WGCDR Chris Cook
Director Preparedness Analysis, VCDF	Ms. Cheryl Durrant
Deputy Director Preparedness Simulation and Modelling, VCDF	Mr. David Oliver
Deputy Director Systems Integration, VCDF	Mr. Vickram Grewal

DSTO

ISR Division	Mr. Glyn Donaldson
Joint Operations Division, S&T Advisor JP2089	Dr. Warren Richer
Chief Information Officer (CIO)	Dr. Tony Hookins
Joint Operations Division – Force Structure Review Support	Dr. Sharon Boswell
Joint Operations Division – Force Structure Review Support	Dr. Nitin Thakur

11. References

ADDP 00.5 2007 — *Australian Defence Doctrine Publication 00.5 - Information Management* (second draft), Defence Publishing Service, Department of Defence, Canberra, ACT, October 2007[29].

ADDP 6.0 2012 — *Australian Defence Doctrine Publication 6.0 – Communications and Information Systems Planning*, Defence Publishing Service, Department of Defence, , Canberra, ACT, 26 June 2012.

ADFP 6.0.1 2012 — *Australian Defence Force Publication 6.0.1 – Communications and Information Systems*, Defence Publishing Service, Department of Defence, , Canberra, ACT, 22 June 2012.

ADFP 6.0.2 2009 — *Australian Defence Force Publication 6.0.2 – Information Exchange*, Defence Publishing Service, Department of Defence, , Canberra, ACT, 13 January 2009.

AGA 2010 — *Australian Government Architecture (AGA)* , Department of Finance and Deregulation, Canberra 2010.

[online] URL: http://agimo.gov.au/policy-guides-procurement/australian-government-architecture-aga/

AGAF 2009 — Australian Government Information Management Office, *Australian Government Architecture Framework*, Version 3.0, Commonwealth of Australia, Canberra, Australia, 2009.

[online] URL: www.finance.gov.au/e-government/strategy-and-governance/australian-government-architecture.html

AGARM 2011 — *Australian Government Architecture Reference Models*, Version 3.0, Commonwealth of Australia, Canberra: Department of Finance and Deregulation, Australian Government Information Management Office (AGIMO), 2011.

[online] URL: http://agimo.gov.au/files/2012/04/AGA_RM_v3_0.pdf

AGIFT 2005 — *Australian Governments' Interactive Functions Thesaurus*, 2nd edition, Commonwealth of Australia, Canberra: National Archives of Australia.

[online] URL: http://www.naa.gov.au

AGIMO 2011 — Australian Government Information Management Office (AGIMO), Department of Finance and Deregulation, Canberra, 2011.

[online] URL: http://www.finance.gov.au/about-the-department/agimo.html

ANSI/EIA 632:2009 — Standard, *Processes for Engineering a System*, Electronic Industries Alliance, Virginia, USA, 2009.

ANSI/NISO — Standard, *Guidelines for the Construction, Format, and Management of*

[29] Although this document is referred to in ADPF publication 6.0.2, the publication is not listed as a formally issued publication on the Joint doctrine Library website at URL: http://intranet.defence.gov.au/vcdf/sites/JointDoctrineLibrary/comweb.asp?page=51864&Title=6 CIS Series.

Z39.19 2005 *Monolingual Controlled Vocabularies*, National Information Standards Organisation, Bethesda: NISO Press, 2005.

BABOK 2009 *A Guide to the Business Analysis Body of Knowledge® (BABOK® Guide)*, Version 2.0, Ontario: International Institute of Business Analysis, 2009.

[online] URL : http://www.iiba.org/IIBA_Website/Professional_Development/Business_Analysis_Body_of_Knowledge_pages/Business_Analysis_Body_of_Knowledge.aspx

Black 2011 *Review of the Defence Accountability Framework*, Australian Government Department of Defence, January, 2011.

BTIAa 2011 *Battlespace Tactical Information Architecture High Level Reference Architecture Book* (draft), version 0.2, Chief Information Officer Group, Australian Government Department of Defence, 17 March, 2011.

BTIAb 2011 *Battlespace Tactical Information Architecture Detailed Level Reference Architecture Book* (draft), version 1.1, Chief Information Officer Group, Australian Government Department of Defence, 13 May, 2011.

BTIAc 2011 *NBA and BTIA Project Guide (*draft), v0.6, Chief Information Officer Group, Australian Government Department of Defence, 2011.

CASAP 2007 *Cross-Agency Service Architecture Principles*, Commonwealth of Australia, Canberra: Department of Finance and Administration, Australian Government Information Management Office (AGIMO).

[online] URL: http://agimo.gov.au/files/2012/04/CAS_Architecture_Principles.pdf

DAF 2005a *Brochure No. 1, Introduction to Enterprise Architecture*, Chief Information Officer Group, Australian Department of Defence, January 2005.

DAF 2005b *Brochure No. 2, The Defence Architecture Framework - A Methodology for Enterprise Architecture*, Chief Information Officer Group, Australian Department of Defence, January 2005.

DCA 2010 *Defence Corporate Architecture (DCA) Reference Book* (draft), Chief Information Officer Group, Australian Department of Defence, 9 August 2010.

DCA 2011 *Defence Corporate Architecture (DCA) Part 1 – A Business View*, Version 1.1 (draft), Chief Information Officer Group, Australian Government Department of Defence, Canberra, ACT, 20 June 2011.

DCDH 2012 *Defence Capability Development Handbook 2012*, Version 1.0, Australian Government Department of Defence, Defence Publishing Service, Canberra, ACT, 2012.

DCP 2012 *Defence Capability Plan Public Version 2012*, Capability Development Group, Australian Government Department of Defence, Defence Publishing Service, Canberra, ACT, 15 May 2012.

[online] URL: http://www.defence.gov.au/publications/CapabilityPlan2012.pdf

DI(N) ADMIN 43-2 2009 Defence Instructions (Navy), DI(N) ADMIN 43-2, *Navy Enterprise Architec*ture, Department of Defence (Navy Headquarters), Canberra, ACT, 10 January 2009.

DODAF 2010 Deputy Chief Information Officer, *The DoDAF Architecture Framework Version 2.02*, U.S. Department of Defense, August 2010.

[online] URL: http://dodcio.defense.gov/dodaf20.aspx

DWP 2009 *Defence White Paper 2009 Defending Australia in the Asia Pacific Century: Force 2030*, Commonwealth of Australia, Canberra: Office of the Secretary and the Chief of the Defence, 2009.

[online] URL: http://www.defence.gov.au/whitepaper

DWP 2013 *Defence White Paper 2013,* Commonwealth of Australia, Canberra: Office of the Secretary and the Chief of the Defence, 2013.

[online] URL: http://www.defence.gov.au/whitepaper2013/

EABOK 2004 Hagan, Dr. P., *Guide to the (Evolving) Enterprise Architecture Body of Knowledge (draft)*. McLean Virginia: The Mitre Corporation, 2004.

FEAF 2007 *FEA Consolidated Reference Model Document*, Version 2.3, United States Government, USA. Federal Enterprise Architecture Program Management Office, 2007.

[online] URL: http://www.whitehouse.gov/omb/egov/fea

Gershon 2008 Gershon, Sir Peter, *Review of the Australian Government's Use of Information and Communication Technology*, Department of Finance and Deregulation, The Australian Government Information Management Office, August 2008.

[online] URL: http://www.finance.gov.au/publications/ict-review/docs/Review-of-the-Australian-Governments-Use-of-Information-and-Communication-Technology.pdf

Hue 2014 Hue, M.A., *An Analysis of SE and MBSE Concepts for Defence Capability Acquisition*, DSTO Technical Report, DSTO Edinburgh, S.A., 2014 .

ICTSTRAT 2009 *Defence Information and Communications Strategy 2009*, Chief Information Officer Group, Australian Government Department of Defence, Defence Publishing Service, Canberra, ACT, July 2009.

IDATAX - no date *Defence Appplication Taxonoloy Review*, Chief Information Officer Group, Government Department of Defence, Canberra, ACT (no date).

[online] URL: http://intranet.defence.gov.au/DRMS/uR4548/AF5556588.pdf

Last accessed 23 April 2013.

IDA BRM 2011 Directorate of Business Architecture, *Integrated Defence Architecture Business Reference Model v1.0*, Chief Information Officer Group, Australian Government Department of Defence, Canberra, ACT, 2011.

IDA TRM 2011 *Technical Reference Model*, Chief Information Officer Group, Australian Government Department of Defence, Canberra, ACT, 2011.

IEEE 1220-2005 Standard, *IEEE Standard for Application and Management of the Systems Engineering Process*, Computer Society of the IEEE, New York, 9 September 2005.

ISO/IEC/IEEE 1471:2000 Standard, *Recommended Practice for Architectural Description of Software-intensive Systems*, International Organization for Standardization, Geneva,

2000.

ISO/IEC 15288:2008 Standard, *Systems and software engineering – System life cycle processes*, International Organization for Standardization, Geneva, 2008.

ISO/IEC/IEEE 42010: 2011 Standard, *Systems and Software Engineering – Architecture Description*, International Organization for Standardization, Geneva, 2011.

JIA 2010 *Joint Intelligence Architecture - Architecture Reference Book*, v1.0 (draft for discussion), Chief Information Officer Group, Australian Government Department of Defence, Canberra, ACT, 7 July, 2010.

King 2010 King, Graham, *The Integrated Architecture: The Models and the Value*, presentation slides, MilCIS, 2010.

[online] URL:

http://www.milcis.com.au/milcis2010pdf/MilCIS2010presentations/1.4b%20-%20Graham%20King.pdf

Knight et al. 2006 Knight, Michele, Vencel, Les, and Moon Terry, *A Network Centric Warfare (NCW) Compliance Process for Australian Defence*, DSTO-TR-1928, DSTO Edinburgh, SA, August 2006.

McDaniel 2012 McDaniel, David, *History of the DoDAF to 2.02*, Proceedings of Workshop for ACT-IAC EA SIG, Architecture & Infrastructure Directorate, Office of the Chief Information Officer, U.S. Department of Defense, 20 July 2012.

[online] URL:
http://www.actgov.org/knowledgebank/newknowledgebank/Events%20Programs%20and%20Initiatives/OSD%20DoDAF%20History%20-%20David%20McDaniel-OSD%2007-20-12.pdf

MODAF 2010 *MOD Architecture Framework v1.2*, UK Ministry of Defence, May 2010.

[online] URL: https://www.gov.uk/mod-architecture-framework

NBA 2020+ 2011 Directorate of Business Architecture, *Networked Battlespace Architecture 2020+ Architecture Reference Book*, Version 1.1, Chief Information Officer Group, Australian Government Department of Defence, Canberra, ACT, 15 April 2011.

Okon 2012 Okon, Walt, *Unified Architecture Framework DoDAF Strategic Direction*, Architecture & Interoperability Directorate, Office of the Chief Information Officer, U.S. Department of Defense, 20 July 2012.

[online] URL:
http://www.actgov.org/knowledgebank/newknowledgebank/Events%20Programs%20and%20Initiatives/OSD%20DoDAF%20Unified%20Architecture%20Framework%20-%20Walt%20Okon-OSD%2007-20-12.pdf

PMBOK 2009 *A Guide to the Project Management Body of Knowledge (PMBOK®) – Fourth Edition*, Project Management Institute, January 2009.

[online] URL: http://www.pmi.org/PMBOK-Guide-and-Standards.aspx

Purcell 2009 Purcell, CDRE Mark, RAN, *Delivery of a Single Enterprise Architecture*, presentation slides, MilCIS, 2009.

[online] URL:

http://www.milcis.com.au/milcis2009pdf/presentations/3.4b%20-%20Mark%20Purcel1.pdf

SEBoK 2012 Pyster, A., D., Olwell, N., Hutchison, S., Enck, J., Anthony, D. Henry and A. Squires (eds). *Guide to the Systems Engineering Body of Knowledge (SEBoK)* version 1.0.1., Hoboken, NJ: The Trustees of the Stevens Institute of Technology ©2012, 2012.

[online] URL: http://www.sebokwiki.org/1.0.1/index.php?title=Main_Page

SF 2010 Strategy Policy Division, *Strategy Framework 2010*, Australian Government Department of Defence, Defence Publishing Service, Canberra, ACT, 2010.

SIE 2010 *Single Information Environment (SIE) Architectural Intent 2010,* Chief Information Officer Group, Australian Government Department of Defence, Defence Publishing Service, Canberra ACT, 2010.

SOA 2011 Instruction No 1/2011, *Service Oriented Architecture*, Chief Information Officer Group, Department of Defence, 4 May 2011.

http://intranet.defence.gov.au/home/documents/data/DEFPUBS/GRPINST/CIO01_11.pdf

SRP 2010 *The Strategic Reform Program Making It Happen*, Australian Government Department of Defence, Defence Publishing Service, Canberra, ACT, 2010.

SWEBOK 2004 Abran, Alain and Moore, James W. (Executive Editors), *SWEBOK Guide to the Software Engineering Body of Knowledge*, IEEE Computer Society, USA, 2004.

[online] URL: http://www.computer.org/portal/web/swebok/

TOGAF 2009 *The Open Group Architecture Framework Version 9 "Enterprise Edition"*, The Open Group, 2009.

[online] URL: http://www.opengroup.org/architecture/togaf/

Z39.19 2005 *ANSI/NISO Z39.19 – Guidelines for the Construction, Format, and Management of Monolingual Controlled Vocabularies*, Bethesda: NISO Press, 2005.

Zachman 1987 Zachman, J.A., *A framework for information systems architecture*, IBM Systems Journal , 26(3), pp 276-292, 1987.

Zachman 2003 Zachman, John A., *The Zachman Framework™: A Primer for Enterprise Engineering and Manufacturing*, e-book, Zachman International, March 2003.

Appendix A: Australian Government Architecture (AGA) Overview

A.1. Enterprise Architecture Concepts

The notion of EA was originally developed in the 1980s as a methodology to aid ICT technologists to better understand the business needs of their organisations and thus to better align ICT investment to support the business needs; typically in the absence of more formalised SW engineering methods.

The approach has since evolved to embrace much wider notions of business process analysis to aid corporate management. EA principally focuses on the business enterprise (i.e. the organisation) rather than the notion of a system, and typically spans people, information, technology and business operations. Since the analysis paradigm is process focussed, it offers few formalisms to consider non-functional aspects relating to the physical implementation (e.g. technological, environmental).

Typically, an EA manifests as a collection of artefacts, comprising lists, drawings, documents and/or models which are used to describe the structure and function of an enterprise in useful ways. Since the EA is inherently conceptual, the architecture descriptions are also typically conceptual in nature, used for communication purposes to support management investment decisions rather than to drive a technical process to implement a specific technical solution.

EA practice can utilise systems thinking, and similar analysis and modelling techniques and tools can be employed as used in operations research (OR), and systems and software engineering. However, the notion of EA is still very young compared to established scientific disciplines, and there is broad variability in EA concepts and application which have yet to converge to an widely accepted and contemporary body of knowledge. The term EA is used in a variety of contexts, both as as a verb and as a noun, including framework, classification schema or taxonomy, methodology, and analytic model (Hue 2014).

A.2. AGA Framework

In 2008 in response to the Gershon Review (Gershon 2008), the Australian Government Information Management Office[30] (AGIMO) within the Department of Finance and Deregulation EA policy and concepts commenced an EA initiative to promote standardisation of ICT infrastructure and processes across whole-of Government. In support of this initiative, AGIMO has developed and mandated use of a set of reference models, collectively known as the Australian Government Architecture (AGA) (AGIMO 2011).

The AGA Framework is a meta-model defining the linkages between five inter-related reference models as depicted in Figure A.1. Collectively, the reference models comprise a framework for describing important elements of the AGA in a common and consistent manner. (AGA 2010)[31].

[30] [online] URL: http://agimo.gov.au/

[31] Information on the AGA reference models can be found on the Department of finance and Deregulation website at URL: http://agimo.gov.au/policy-guides-procurement/australian-government-architecture-aga/aga-rm/2-reference-model-overview/

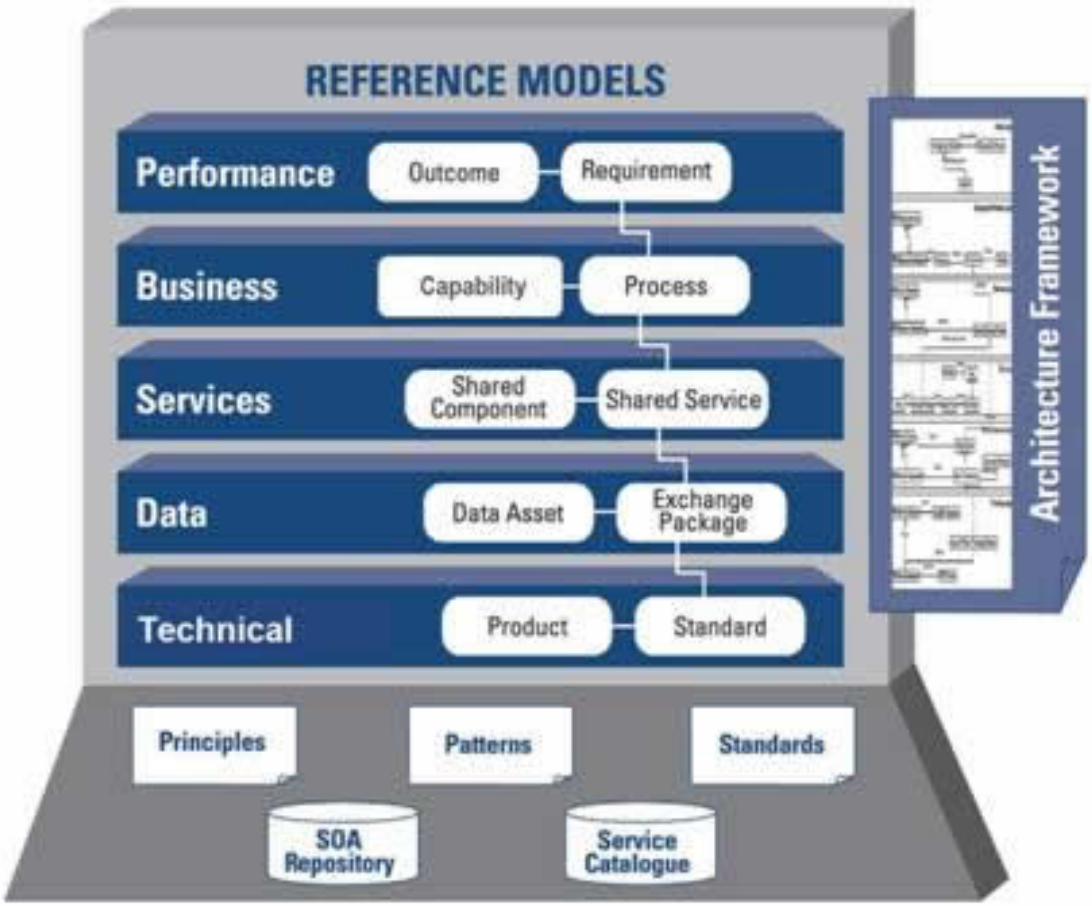


Figure A.1. Australian Government Architecture (AGA) Reference Model

The AGA meta-model comprises five more detailed reference models as follows:

1. ***Performance Reference Model (PRM)***

   The PRM is a performance measurement framework providing common output measurements across whole-of-Government. This is to facilitate agencies to better manage the business of government at a strategic level by providing a means for using an agency's enterprise architecture to measure the success of ICT investments and their impact on strategic outcomes.

   The PRM seeks to achieve these goals by providing a common language by which respective agencies can describe their outputs and measures used to achieve programme and business objectives. The model articulates the linkage between inputs, internal business processes and activities, and the achievement of business and customer-centric outputs and outcomes. The intent is to facilitate resource allocation decisions based on comparative determinations on which programmes and organisations can most efficiently and effectively deliver those outcomes and outputs within a whole-of-Government context.

2. ***Business Reference Model (BRM)***

   The BRM provides a framework for facilitating a whole-of-government functional view of the Government's Lines of Business, independent of the agencies performing them. It is

structured into a tiered hierarchy representing the collective business functions of whole-of-Government, Business areas are listed at the highest level, then broken down into lines of business that are comprised of a collection of business capabilities at the lowest level of functionality in the BRM.

At an agency level, business capabilities are represented by business services that are enacted through the business processes created by the agencies, which in turn, described in the Service Reference Model.

3. ***Service Reference Model (SRM)***

   The SRM provides a business-driven, functional framework to classify services according to how they support business and performance objectives.

   Service areas are classified independent of business function within the SRM to provide a foundation for sharing and re-use of business services, applications, application capabilities and components pertaining to ICT investment and assets.

4. ***Data Reference Model (DRM)***

   The DRM is a standards-based framework to enable information sharing and re-use across whole-of-Government by using standard description and discovery of common data and through the promotion of uniform data management practices.

   It seeks to provide foundational guidance for implementation of repeatable processes to enable data sharing in accordance with government-wide agreements, while allowing agencies to use multiple implementation approaches, methodologies and technologies.

5. ***Technical Reference Model (TRM)***

   The TRM is a technical framework categorising technical standards and technologies to provide a foundation to advance the re-use and standardisation of "best-fit" technology and services to support their business functions and thereby benefit from economies of scale.

   It seeks to provide a common, standardised vocabulary to facilitate inter-agency discovery, collaboration and interoperability.

The Reference Models draw upon five additional concepts including:

- Design Principles;
- Design Patterns;
  - These are archetypical solutions to recurrent design problems that reflect well-proven design experience.
- Standards;
- SOA Repository; and
- Service Catalogue Repository Service (AGARM 2011).

A.3. Business, Enterprise and Architecture Definition Quandary

Having a common understanding of the basic concepts in the Australian Government context is fundamental to the whole-of-Government enterprise architecture approach.

Enterprise architecture is defined in the AGA Reference Model as "the explicit description and documentation of the current and desired relationships among business and management processes and information technology." To provide different temporal perspectives, terms

'current architecture' and 'target architecture' are used to describe the rules, standards, and applicable systems life cycle information for an agency to manage its ICT portfolio as it transitions from its current state to a future target environment (AGARM 2011).

The definition of business in the AGA context is somewhat circular, in that it defines the term "business" in terms of the people and organisations that are described in the Business Reference Model (BRM) (AGARM 2011). It also provides clarification drawn from the "Universal Description, Discovery and Integration" standard where business is referred to in the context of business Entity. The BRM in turn, refers to explicit functions of Government at a whole-of-Government level, independent of government agency structures. The AGAF infers that the term "business" equates to whole-of-Government functions, performed by the Government, which is citizen-centric, results-oriented and market-based.

However, there are many different definitions of business used concurrently across the broader Australian Stakeholder community, some of which are organisation-centric rather than function-centric, and these differences will remain pervasive[32]. It is of paramount importance therefore to be both explicit and consistent with use of vocabulary for AGA purposes.

Numerous terms in the AGARM have specific contextual meaning. Specific effort has been applied to align with the definitions published in the Australian Government Interactive Functions Thesaurus (AGIFT 2005), which provides a three-level hierarchical thesaurus that describes business functions carried out across Commonwealth, state and local government in Australia to maintain consistency of language throughout government publications. However, the descriptors are very high level and do little beyond identifying that Army, Navy and Air Force are part of the Australian Defence Forces.

Many of the definitions of terms used within the AGA have been drawn from ANSI/NISO Z39.19 – Guidelines for the Construction, Format, and Management of Monolingual Controlled Vocabularies. This standard is extensively used by libraries to index databases for database search purposes.

Definitions are provided in the AGAF for key terms including:

- ***Interface***
  - the capabilities of communicating, transporting and exchanging information through a common dialogue or method.
- ***Interoperability***
  - the capabilities of discovering and sharing data and services across disparate systems and vendors.
- ***Integration***
  - the software services enabling elements of distributed business applications to interoperate. These elements can share function, content and communications across heterogeneous computing environments.

[32] For example, the BABOK Guide, produced by the International Institute of Business Analysis, does not offer a specific definition of the term business. However it defines business analysis as the set of tasks and techniques used to work as a liaison among stakeholders in order to understand the structure, policies and operations of an organisation, and recommend solutions that enable to organisation to achieve its goals. Organisation is defined as an autonomous unit within an enterprise, operating on a continuing basis, under the management of a single individual or board with clearly defined boundaries that work towards common goals and objectives. Enterprise is an organisational unit, organisation, or collection of organisations that share common goals and collaborate to provide specific products or services to customers. Enterprise architecture is defined as a description of an organisation's business processes, IT software and hardware, people, operations and projects, and the relationships between them. (BABOK 2009).

- ***Hardware/infrastructure***
  - the physical devices, faculties and standards providing the computing and networking, within and between enterprises.
- ***Modelling***
  - the provision of support for the process of representing entities, data, business logic and capabilities, for aiding in software engineering.
- ***Computer/Telephony Integration***
  - supports the connectivity between server hardware, software and telecommunications equipment, into a single logical system.
- ***ICT***
  - is used in the context of exchanging information and communication pertaining to the commercial telecommunications industry (AGAF 2009).

Significantly, these definitions are not generic as might be found in a general purpose dictionary such as the Webster dictionary, but are tailored to suit the enterprise-centric and information specific context of the AGAF. For example, the Webster online dictionary defines the term *interface* variously as:

- a surface forming a common boundary between two bodies, spaces, or phases;
- the place at which independent and often unrelated systems meet and act on or communicate with each other;
- the means by which interaction or communication is achieved at an interface;
- to connect by means of an interface; and
- to interact or coordinate harmoniously [33].

Notably absent from the AGAF are definitions for terms with both engineering and business significance such as architecture, system, component, service, and enterprise.

- [33] [online] URL: http://www.merriam-webster.com/dictionary/interface.

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. DLM/CAVEAT (OF DOCUMENT)

2. TITLE

A Review of Enterprise Architecture Use in Defence

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Meredith Hue

5. CORPORATE AUTHOR

Defence Systems Integration Technical Advisory
Joint and Operations Analysis Division
Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-3040	AR-016-127	Technical Report	September 2014

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2014/1123432/1	ERP 07/369	CSIO	75	58

14. RELEASE AUTHORITY

Chief, Joint and Operations Analysis

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for Public Release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DSTO RESEARCH LIBRARY THESAURUS

capability development, methodology, systems engineering, complex systems, enterprise architecture, operations research

19. ABSTRACT

This report provides a retrospective analysis of enterprise architecture practice in Defence over the last decade leading to the establishment of the Integrated Defence Architecture. A review was undertaken to gain insight into the perceived value that various Stakeholders within Defence were realising from the use of enterprise architectures to assist with the realisation of the integrated networked force. The report distils lesson learned over this period and provides a benchmark to evaluate the effectiveness of subsequent enterprise architecture practice in Defence. The impetus for enterprise architectures and the modus operandi were also examined to provide context to the review findings.