Assigned Number: I-112

11TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM

Coalition Command and Control in the Networked Era

Title: NCW Risk Assessment – Towards a Compliance Policy and Process

Topics: Policy, C2 Architecture, Network Centric Metrics

Warren Richer, Elizabeth Kohn, Gina Kingston

Point of Contact:
Warren Richer
DSTO

Department of Defence
Canberra, ACT 2600
AUSTRALIA
+61 2 6256 6315 / +61 2 6256 5233
warren.richer@dsto.defence.gov.au

NCW Risk Assessment - Towards a Compliance Policy and Process

Abstract

The Australia Defence Force (ADF) has adopted the *Network Centric Warfare* (NCW) concept as a key driver for transitioning to a fully networked force capability by 2020. Defence has made a commitment to Network Centric Warfare (NCW) (ADF 2004, 2005). They are now in the process of developing mechanisms to ensure that projects have the requisite ability to integrate into the future networked force. In 2005 DSTO developed a framework for compliance—now termed the NCW Risk Mitigation Review (RMR) framework—for the NCW Program Office (NCWPO). The NCWPO have adopted some elements of the NCW-RMR framework as part of their NCW compliance process.

This document is the *First* of two being presented to this forum and describes the three RMR supporting views namely *systems, process and assessment.* This paper contextualises the problem space, reviewing the current process, identifying problem areas and stakeholders involved before outlining the NCW RMR framework. The paper describes various *systems* approaches employed to better understand the NCW integration problem space and how some of these findings were used inform the development of a more *generic approach* to NCW compliance. The *Second* paper, (Kingston et al 2006) describes the theory and philosophy behind this framework.

Introduction

The Australia Defence Force (ADF) adopted the *Network Centric Warfare* (NCW) concept (DoD 2002; DoD 2004) as a key driver for employing the future warfighting concept,[1] and assisting Defence in achieving future military strategic objectives through a transition to a fully networked force capability by 2020 [2]. In December 2004 the Defence Minister officially released the aspirational *NCW Roadmap*[3], which serves as the capstone guidance on how the ADF will achieve such a transition to a fully networked force in the timeframe described.

The Chief of Capability Development Group (CCDG) was made responsible for ensuring the ADF develop a comprehensive program to achieve this vision of a future *network-centric* force. To support the transition[4] two teams were raised under Capability Development Group (CDG) namely:

- The NCW Implementation Team (NCWIT) was raised under a Head Capability Systems (HCS) (2 star).

[1] ADDP-D.3. The Future Warfighting Concept, 2003 an ADF booklet released in 2003 by the Chief of Defence Force, General P.J Cosgrove, AC MC. Which articulated the ADF's new warfighting concept of *Multi-Dimensional Manoeuvre.*

[2] ADF Booklet, *Force 2020*, released in 2002 by the Chief of Defence Force, Admiral C.A. Barrie which provided initial guidance on how to progress the Defence force towards the future world of 2020.

[3] The *NCW Roadmap* of 2004 and a more recent version released late 2005 is designed to provide initial steps and direction on how the ADF could discover and exploit the opportunities of Network Centric Warfare by detailing the long term goals (target states) for developing the ADF's warfighting capability out to 2020.

[4] Ibidem *NCW Roadmap.*

- The NCW Program Office (NCW PO) was raised under the Director General Integrated Capability Division (DGICD) (1 star).

The Implementation Teams task was to manage and coordinate activity related to the implementation of the *NCW Roadmap*, which included:

1. *Establishing an NCW implementation strategy the ADF should achieve.*
2. *Establishing the Network by addressing the core and supporting infrastructure upon which the network will be developed.*
3. *Address the human dimension of a networked force initiating changes with appropriate support.*
4. *Accelerate the process of change and innovation in capability development through such initiatives as Rapid Prototyping, Development and Evaluation (RPDE)*[5].

The NCW PO's initial task was to develop an NCW *integration plan* to guide future projects towards achieving the desired level of *integration* through the adoption of an NCW compliance framework across the *Capability Life Cycle (CLC)*. This *integration plan* is to be progressively introduced into the Defence capability planning process over the next 12-18 months.

In October 2005, the NCWPO was provided a draft NCW compliance framework designed to support the Capability Developments Group's *integration plan.* The framework is based on a risk mitigation model designed to assess the level of risk to Defence of a project not realising its full NCW potential. The model was developed by the research team[6] supporting the NCWPO.

Purpose

This is part *One* of *Two* papers being presented to the 11th ICCRTS with the second covering the theory (Kingston, Richer et al. 2006) underpinning the risk assessment framework. Part *One,* describes a NCW Risk Mitigation Review[7] (RMR) framework proposed to the NCWPO, describing the three views namely *systems, process and assessment.* This paper provides the foundation for Part *Two.* The paper is structured as follows:

- *Bounding the problems space.* Here the paper reviews current capability development and acquisition processes within the context of the *capability life cycle* and employs a *systems enterprise model* to support the initial development of NCW question lists, then identifies the key *NCW acquisition problems.*
- *Identifying stakeholders.* This involves reviewing the stakeholders and responsibilities across the *capability life cycle* through the lens of various *systems strategies and methodologies* to inform an integrated systems approach to *capability development and acquisition* for the future force package.

[5] RPDE is a capability raised by Defence and is a consortium of Industry and Defence specialists aimed to support CCDG by addressing NCW capability shortfalls and identify and evaluate solutions in the near term. http://www.rpde.org.au/

[6] The model was developed by the team members of the Systems Enablers for Future Warfare (SEFFW) task within the Defence Systems Analysis Division (DSAD) a division of the Defence Science and Technology Organisation (DSTO).

[7] The framework and process adopted by Defence as the NCW Compliance Process which was recently incorporated in the Defence Capability Development Manual (DCDM) (The Blue Book) 2006.

- *Developing an assessment framework.* Here the paper outlines the work in developing the NCW RMR framework and process and provides details on the model and follow-on activities.

The paper draws from other research activities over the last twelve months the results of which form a systems approach to high level considerations for meeting NCW compliance needs across the *capability development and acquisition (CD&A)*[8] *process*.

Contextualising the Problem Space

As stated previously, the ADF is committed to Network Centric Warfare (NCW) (DoD 2005) to, amongst other things, address the issues of what could be referred to in capability development as a *projects-centric* approach, where cross project integration is pursued if critical to that project in an CD&A environment where NCW integration policy, direction and guidance is still maturing.

As part of its commitment to NCW, the ADF is now moving from a *projects-centric* approach, to one where cross project integration issues are considered.

The transition from the current *project-level* approach to *capability development and acquisition* to *force-level (systems-of-systems) approach* to achieve the desired level of future capability doesn't come without its challenges. The absence of any *force-level approach* to integration impacts on all projects in the Defence Capability Strategy (DCS) including those planned to meet the requirements of:

- *current force-in-being* integration needs (0-3/5 years),
- projects in the pipeline for meeting the needs of the *enhanced force* (3/5-15 years or referred to as 2015), and
- CD&A future forecasting needs for the *future-force* requirements (>15 years referred to as 2020 and 2030)

Leveraging just a *systems engineering approach* using techniques such as architectures and standards can be restrictive if there is no architecture and the standards don't exist for the epoch of delivery to support the capability package under design at the time. Such challenges are not by any means new and not just restricted to the design of a future joint force but also to a force which has wider coalition and multinational operational interface implications.

The Defence Capability Life Cycle Process

To appreciate the level of complexity involved in a CLC requires a need to reflect on the capability development process in Defence Capability Manual[9] (DoD 2006). The Capability Life Cycle incorporates five phases as detailed in figure 1.

[8] Capability Development &Acquisition (CD&A) for this paper is defined as "those phase two and three activities of the five-phased Defence capability life cycle (CLC) which include defining the *Requirements* for future capability and the *Acquisition* and procurement of the Government endorsed solution to meet the identified requirements. This is discussed further under CLC.

[9] Defence Capability Development Manual (DCDM) 2005 and supporting directives were the principal CDG documents used in the study. The DCDM 2006 edition is now the version available for public release at www.defence.gov.au/**capability**/_pubs/dcdm%20(2006).pdf

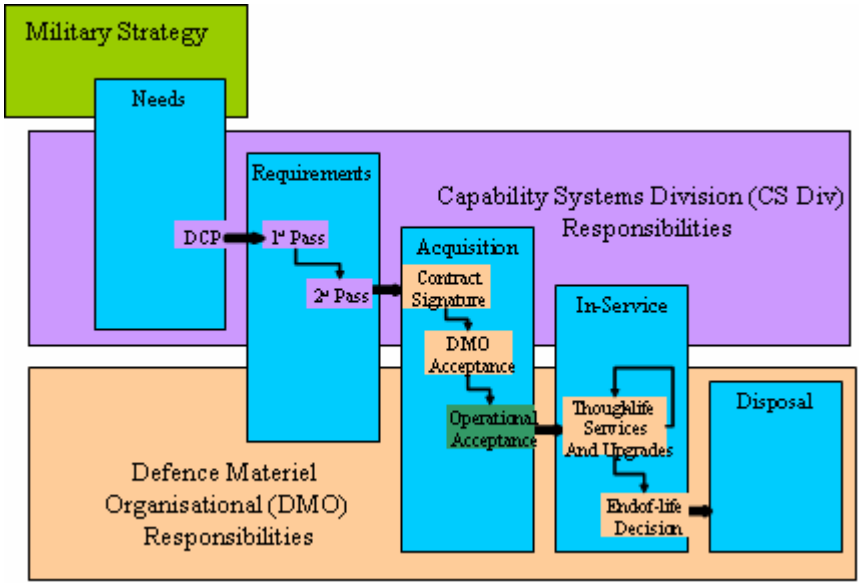

Figure 1 The Defence Capability Life Cycle.

The two main groups within the CLC are as follows:

- the Capability Systems Division (CS Div)[10], the overseer for Chief Capability Development Group (CCDG)the prime Defence Customer, and
- the Defence Materiel Organisation (DMO) as the prime Defence Supplier.

This means that there will be involvement from both parties throughout a project's lifecycle. In Figure 1 activities that are lead by CS Div are shown in purple, while those conducted by the DMO are shown in orange. The process focuses on Capabilities which, for the ADF means the capacity to achieve an operational effect. Each Capability is packaged neatly and flows through the committees on its own merits.

The Five Phases Approach

1. The Needs Phase – Here Defence based on strategic guidance, future operational concepts and proposed force structure *identifies capability gaps and proposes technology options for further study to fill the need*. The Needs Phase concludes when Government endorses the need and approves the inclusion of the project into the Defence Capability Plan.

2. Requirements Phase – Requirements phase incorporates a two pass process:

a. *First Pass* – 1st pass approval sets the capability boundaries for solutions considered at 2nd pass. 1st pass approval is, in effect, approval in principle to proceed with more detailed analysis and costing of Government approved option(s).

b. *Second Pass* –2nd pass approval is formal approval by government of a specific capability solution to an identified capability development need.

3. Acquisition Phase – Closure of the Requirements Phase represents a contract between CDG and the DMO for the delivery of capability and the start of the

[10] CS Div responsibilities include amongst other things, the oversight of the Defence Capability Plan (DCP), the review of all cost estimates associated with unapproved major capital projects and the development of new proposals in response to identified capability gaps and changes in the strategic guidance.

Acquisition phase. During this phase a successful contractor builds the system to meet the capability gap.

4. In-Service Phase – From the release of the *final operational capability* (FOC) and accepted-into-service the capability is managed through Service Level Agreements from a capability system and life cycle perspective which includes upgrades and maintenance throughout the life-of-type (LOT) of the capability. Responsibilities for LOT are dispersed and shared across the Australian Defence Organisation (ADO)[11].

5. Disposal Phase – The capability system as a whole is withdrawn from service and disposed of or redeployed, depending on the nature of the individual capability input.

Capability Development & Acquisition as an Enterprise

In order to move forward it is necessary to place the requirement for *Network-centric* compliance in context to establish a suitable model from which to progress further research. Defence Capability Development and Acquisition (CD&A) includes CDG, Chief Information Officer Group (CIOG), Defence Science and Technology Organisation (DSTO), the prescribed agency DMO,[12] and Defence Industry. They holistically could be described as an enterprise or coalition of Defence and Industry stakeholders, all with different and sometimes competing interests as well as different perceived solution to Defence capability development issues.

It is now mandated within Defence that all new projects within CD&A must comply with the architectural principles and guidelines of the Australian Defence Information Environment (DIE)[13] (DoD 2002) governed by the CIOG[14]. Currently a problem exists where future projects with a delivery beyond 2010 cannot guarantee the stability of current architectural guidance to develop their products and in the absence of any future NCW architecture for such epochs they have to rely on other methods to ensure any realisation of integrated force level NCW capability at the time of future delivery.

It is accepted that these architectures, based on the original *Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Architecture*

---

[11] However, there is a need to identify sufficient governance is in place to ensure those NCW capabilities delivered into service are sustained, by regularly checking that an NCW capability has not degraded.

[12] In July 2005, Defence Materiel Organisation (DMO) became a prescribed agency accountable directly to the Minister for Defence iaw the Financial Management and Accounting Act 1997 while remaining accountable to the Secretary of Defence and Chief Defence Force for administration under the Public Service and defence Acts. Further details available at http://www.defence.gov.au/dmo/

[13] The DIE is a capability that consists of the information used by Defence and the means by which it is created, managed, manipulated, stored, disseminated and protected. Defence's information can be regarded as falling within one of four Information Domains: management, command support, intelligence and electronic warfare, and surveillance. Defence's Information Domains (DID) are supported by the Defence Information Infrastructure (DII) comprising software, hardware and other information communications technology. Together they form the DIE. The DIE does not include the sensor or weapons systems that provide information to and utilise information from the DIE.

[14] Amongst other roles, Chief Information Officer Group, provides Defence architecture standards support to CDG and is responsible for overall information management within the DID.

Framework (C4ISRAF) (US DoD 1997), are the endorsed models for describing military systems from a systems or network perspective, however, as inferred by (Cook 2000) in order to gain a thorough insight into the information-rich military enterprise the chosen C4ISRAF, in this case the DIE, should be used in conjunction with appropriate systems enterprise models. To assist in bounding the problem the authors initially drew upon the MIT 90[15] model which is widely used within Defence and Industry as an enterprise model for analysing the core components of a technically and strategically focused enterprise.

For the *Network-centric* problem space, MIT 90 is of benefit when broken down to its constituent parts, as it recognises the importance of information technology as a fundamental component of the model. It integrates well with the ADO *fundamental inputs to capability* (FIC)[16] (DoD 2006) as it address those core areas of management processes, enterprise structure personnel interfaces including roles and skill issues while additionally recognising the importance of the technological and socio-economic environmental pressures and influences, which on the surface FIC does not appear to address well.

MIT90 "Five Forces"

MIT90 framework comprises five interacting "forces" where each force is in constant motion reacting to or impacting on other forces within the model while at the same time responding to the pressures of the external environments such as in this case the adoption of NCW Integrated approach to CD&A. The descriptors below have been adapted from the original version (Scott Morton 1991) using the *NCW Roadmap* (DoD 2005) guidance to realize an MIT 90 framework more suited to the current NCW environmental context.

MIT90 Force Descriptions

- ***Technology:*** Includes the communications and network standards, architecture, core and supporting infrastructure, enterprise wide systems networking, the level of technical and systems interconnectedness achievable based on the conformance to the systems concepts and implementation strategies to realize the projects *NCW Roadmap* target states.

- ***Individuals and roles:*** Concerned with the human dimension of an NCW enterprise, the skills required for the tasks they undertake, and the level of education and training they require to perform their functions in a *Network-centric* environment (Warne, Irena et al. 2004). This force recognizes that there will be a blurring of job categories and tasks in an NCW enabled enterprise. Any progress in the development of networks and networking processes must be done cognizant of the impact on the human dimension.

---

[15] **M**anagement **I**n **T**he 90s (MIT90) research program was created in 1984 to examine the impact of information technology on organizations of all kinds [(Scott Morton, 1991) Cook, S., J. Kasser, J., & Burke, M., 2000, *Assessing the C4ISR Architecture Framework for the Military Enterprise*, Systems Engineering and Evaluation Centre, University of South Australia.
2000]. The research program led to the development of the MIT90 enterprise framework, that has provide useful in considering the impact of information technology on organizations.

[16] **F**undamental **I**nputs to **C**apability are those essential elements that must be considered and changed accordingly to realize the full potential of the capability in service and include personnel, organisations, collective training, major systems, supplies, facilities, support and command and management.

- ***Structure:*** Recognizes that in an NCW enabled enterprise the organisational structures will change and new dynamic and agile organizational structures will be adopted in order to leverage maximum benefit from this *Network-centric* paradigm (Alberts 2003). In order to meet such demands the enterprise must ensure that governance is transparent across the capability systems of systems lifecycle.

- ***Management processes:*** In line with the enterprise strategy the management processes must be aligned to support such changes to guarantee the realization of the benefits of *Network-centric* enablers throughout the CD&A program. More agile and dynamic management practices are called for to enable projects to move forward more rapidly to meet NCW requirements and at the same time reduce the risk of introducing legacy capabilities.

- ***Strategy:*** This is the enterprise strategic business model (CD&A), informed by guidance from government and military strategic tool sets and adapted operational concepts, in the pursuit of Defence goals and tasks articulated in the latest *NCW Roadmap and NCW Strategic guidance* and refined in supporting guidance. Given that adversaries and competing organizations will also exploit *Network-centric* strategies, agile and innovative approaches are needed to generate appropriate and timely outcomes to achieve the intended strategic effect or to seek/maintain a competitive initiative and advantage.

Since the formal adoption of the *NCW Roadmap* in December 2004 there has been a degree of debate within the ADO and the wider Defence community, as to just what NCW looks like in the Australian context as considered by (Borgu 2003) and more importantly, just what a *network-centric compliant* force looks like. These and similar questions are not new nationally or internationally as (Kaufman 2004) has explained. Here we employed the revised MIT90 framework to the NCW problem space to initially capture some high level issues detailed below and categorise some of the questions raised which are detailed at Appendix A. These formed the high order master list for reference throughout the study.

The following statements represent a broad view of the enterprise NCW problem space as follows:

1. *The current whole of DCP process does not address the NCW requirements for the future force.*
2. *There is a need for the integration of NCW requirements and compliance framework into a whole of CD&A program approach.*
3. *NCW compliance of all future capability and development projects will impact on the current and planned Defence C4ISRAFs and the Fundamental Inputs to Capability (FIC).*
4. *The responsibilities of integrating NCW compliance into the CLC will impact on all stakeholders, contributors, witnesses and affected parties of the Defence CD&A*[17].
5. *There is no endorsed aspirational NCW architectures to inform and guide CD&A future planning across chosen epochs.*

[17] What is currently unknown with the new ADF strategy of adopting an NCW approach to warfighting for all future capability: a. the impact on the ADO and CD&A process, b. the cost of NCW capability across the FIC, and c. the increased level of risk management and mitigation.

6. *Establishing an NCW assessment framework prior to such architectures demands a more holistic approach to NCW compliance.*

NCW Acquisition Problems

Initial research into developing and integrating NCW compliance capability across the CD&A revealed a number of perceived problems in the acquisition of NCW. Time and resource limitations on the team meant that a qualitative approach to identifying the issues was taken with problems identified through discussions with approximately 15 selected experts rather than through an intensive literature review or consultation process. These experts included researchers, who have worked in the field of NCW before it became the policy of the Australian Defence Force, as well as military personnel concerned with the acquisition of NCW systems. These discussions were informal in nature, and so problems have not always been associated with specific sources. However, most of these problems were identified by multiple sources. The key issues identified were:

- difficulty in justifying NCW aspects of a project,
- delivery of the NCW capability and
- the ability to use the NCW capability on delivery,

These are issues are discussed further below.

Acquiring a *leaning by doing* capability

Perhaps the biggest problem with the acquisition of NCW within the ADO at the current time is the lack of consensus what it is and how then to implement it. This stems from two sources – the *first* is the uncertainty over the model of NCW that will be adopted by Australia. Several models of NCW exist – with different levels of fidelity or detail. (Alberts 2003) from the US have proposed a model based on shared situation awareness – the philosophy of getting the right information to the right people at the right time. (Scholz and Lambert 2005) have proposed a model based on local decision making – *Ubiquitous Command and Control or UC2.* While (Dekker 2006) has considered how networking the force can enable centralisation or decentralisation – and has provided some insights into when each might be appropriate. Australia has not committed to any of these models, nor has it identified when each might be appropriate. Instead Australia has chosen to take a *learn by doing* approach (DoD 2004). This is understandable given the dearth of information on which to base a decision[18].

Articulating how NCW adds to your fighting power

As a consequence of adopting this *learn by doing* philosophy, there is very little information to assist implementers in deciding which, why and how systems should be integrated. Does this *learn by doing* philosophy sit within the context of long project gestation periods? Furthermore, proposed approaches to assist implementers, such as the use of architectures, themselves require an analytical basis from which to draw. This results in problems articulating the benefits of NCW projects or the NCW

[18] This statement applies equally well to the generic models of NCW and to the considerations of specific situations – such as when to centralise or decentralise and when to favour performance over agility – with a few notable exceptions (such as Dekker, A. (2006). " Measuring the Agility of networked Military Forces." The Journal of Battlefield Technology 9 (1): 19-24 and Perry, W. Button, R. et al. (2002). Measuring of Effectiveness for the Information – Age Navy. Santa Monica, RAND.

aspects of projects, which are exacerbated by the project-based acquisition processes currently used by Defence (DoD 2006). However, this leads to the first problem notably:

NCW Issue 1. *NCW aspects of projects are difficult to justify, despite the Department's focus on NCW .*

Project –Based Capability Development & Acquisition

In the current project-based acquisition projects are generally approved and managed on an individual basis, which is often driven by financial concerns or individual capability requirements. Dependencies between projects and capabilities provided through multiple projects are difficult to comprehend and contemplate when focusing on one project at a time. Such projects – NCW projects – are often delayed when facing decision-making committees. The focus of the acquisition process on individual projects also has potentially severe implications when it comes to the implementation of systems. This highlights the second problem notably:

NCW Issue 2. *NCW aspects of projects often fail to combine to deliver an integrated NCW capability*[19].

Acquisition unprepared for rapid technology change

For a majority of major capability development projects being locked into the current acquisition cycles of five to seven years or longer, technology will continue to change at a rate that outpaces our ability to acquire the latest (Alberts, 2003). There is a large number of interrelated projects progressing through the acquisition process in parallel, which highlights the complex nature of CD&A particularly as these new capabilities approach delivery dates for acceptance into service. Even after a comprehensive set of projects have been identified and suitable deadlines established, problems can still arise (DoD 2003)[20] in the specification and delivery of the systems. The US Net-centric checklist (Shekmar and Kreger 2004) is trying to address this problem, in part through the specification of standards. However, rapid technological change (Alberts 2003) means that it is difficult if not impossible to specify standards prior to acquisition that will be sufficient at acceptance – let alone throughout the life of the system. This means that a project may be approved and delivered before the infrastructure upon which it depends, and that there may be capability gaps – such as gateway service providers – in the NCW capability delivered. This now leads us on to the third issue namely:

NCW Issue 3. *Projects could fail to deliver an NCW capability that can be used upon delivery due to the absence of:*

NCW Sub Issue a. *major systems which are delivered late, and*

NCW Sub Issue b. *other fundamental inputs to capability not being considered.*

Based on the discussion so far it can be assumed that whatever compliance assessment capability is introduced it must at the minimum be able to address a broad range of NCW compliance and integration issues e.g. as detailed in the previous section and at figure A1. Similarly the capability should be able to address

---

[20] As reported in the public release of the *Defence Procurement Review* (Kinnaird Review) 2003, "…continuing delays in the delivery of major defence equipment means that the ADF has failed to receive the capabilities it expects…"

issues raised in the modified *five force descriptors* of MIT90 model, the example questions resulting from the initial analysis of the revised model at Appendix A and more immediately the three key *NCW issues* raised above. In summary, the process must ensure that:

- projects adequately justify the NCW capability,
- those projects defining the technologies communicate with those that are using the technologies,
- the technologies are in place when the capability comes into service, and
- all stakeholder agreed expectations are met upon delivery.

These will be difficult to address while each project can make its own implementation decisions, as projects can make inconsistent choices potentially resulting in the delivery of a capability that does not meet the needs of any NCW model or client. Defence is trying to address this problem through the establishment of oversight boards, such as the NCWPO and Electronic Systems Integration Configuration Management Board (ESI CMB) (DoD 2006) and the ADF Tactical Integration Authority (ADFTA) however, these boards still require a process to implement.

NCW Integration Stakeholders and Responsibilities

Relationship to System Thinking

Arguably, from a systems perspective, the MIT90 enterprise model as articulated by Cook et al, (2000), describes the enterprise as a dynamic *open system*, inferring, from a metaphorical perspective, the organic or *a learning system*, i.e. brain metaphor (Flood and Jackson 2002). As an enterprise model, it can be equally argued that it describes a *complex* enterprise as a system of numerous and diverse business units displaying *coalition* or even *political* metaphorical attributes with *pluralist* issues as it is designed to recognise the existence, of and interact with, the ever changing external environment.

On the other hand, CD&A as an enterprise or continuing on with the systems approach, has to deal with *complex pluralist* and sometimes *coercive* issues as it is continually influencing as well as being influenced by numerous internal issues as well as those external domestic and international industrial and financial environments. Additionally, the CD&A enterprise is made up of many cross organisational business units which are required to exchange services and meet responsibilities not only across the capability development enterprise but across Defence as well as external agencies. Though CD&A employ project management style processes suggesting more a *hard systems* approach along *systems engineering (SE)* lines, there is the need for a dynamic *open system of systems* approach employing suitable systems methodologies. The following details the approach taken to better understand the problem space and to support this area of research.

Putting Systems Methodologies to Work

This section involves the investigation of enterprise stakeholder and coalition groups within this CD&A enterprise and the boundaries associated with such a complex organisation. The approach taken was to investigate these issues through the lens of suitable systems methodologies.

The Total Systems Intervention Tool Set

The method used to identify suitable systems tools was the (Flood and Jackson 2002) Total Systems Intervention (TSI) methodology as described in Appendix B. The outcome of the TSI approach was the adoption of the Ulrich (1987), Critical Systems Heuristic (CSH) checklists and Churchman's (1970) Boundary Critique methodology. The following section briefly captures the core issues that led to this decision.

The selection of these systems tools was due to the direct result from applying TSI. Here the TSI framework identified the CD&A enterprise as actually bordering between *complex-pluralist* and *simple-coercive* methodologies for the following reasons:

- CD&A is constantly dealing with multilayered and complex issues to meet enterprise goals across a pluralist or coalition of players who are trying to impose their political or favoured strategies to also meet individual capability/project level goals i.e. a *complex-pluralist to coercive* environment.
- CD&A is responsible for the CLC of a defence capability.
- CD&A responsibilities internally interchange as the capability moves from concept to options to solution, in-service acceptance to disposal and, as such, involve a diverse number of stakeholders, coalitions and contributors each with sometimes differing strategic and operational goals.
- The CD&A program includes many extremely complex and expensive major as well as minor projects each with diverse issues, competing aims and dependencies, e.g. time-sensitive delivery of dependent, supporting or parallel capabilities.
- Many stakeholders come to the table with project and political baggage, e.g. underlying and diverse *capability as well as platform-centric* views to joint force projects.
- Attempts to establish an NCW compliance framework will be subject to all these issues including the internal politics between major stakeholders during the design, development and implementation stages, e.g. responsibility for the delivery of appropriate common tool sets (architectures and standards); the responsibilities for assessing options, the selection and then acquisition of an appropriate solution (balancing capability with cost, realising value for dollar at national expense); and the acceptance testing to amongst other things realise a projects NCW capability.

Ulrich, CSH methodology (Midgley, Munlo et al. 1998) and Churchman's (1970) boundary critiques method were used together to review the stakeholders and boundaries of CD&A. Ulrich's methods attempt to draw out stakeholders, through the application of a series of boundary questions to establish the client, the decision-maker, the designer and the witness. Churchman's boundary critique method in turn helps to establish the stakeholder groups and there boundaries. Employed together these methodologies provide answers to questions relating to CD&A stakeholders their boundaries and identify and inform responsibilities which inturn inform guidance for the systems design. The applications of both methodologies are detailed at Appendix B & C.

Outcomes from CSH and Boundary Critique Methods

The boundary critique diagram at Figure 2 captures the results of data collected in the application of the CSH boundary questions as detailed at Appendix C. The process identified that the *stakeholders and contributors* of a Defence capability

development and acquisition process are many, ranging from a number of programs, divisions, specialists groups, committees and business units each with numerous levels of accountability in any one or more of the five phases of a CD&A as detailed at Figure 1.

These stakeholders and contributors extend across many *functional area*s of the Australian Defence Organisation (ADO) and Government agencies including: strategic policy, finance, science, defence capability development, acquisition & material, international and national standards authorities, industrial law and contract management, technical authorities, test & evaluation authorities, human resources including manpower, training and occupational health & safety, and finally across organisational initiatives such as Rapid Prototype Development & Experimentation (RPDE), Rapid Acquisition; and Concept Development And Experimentation (CD&E).

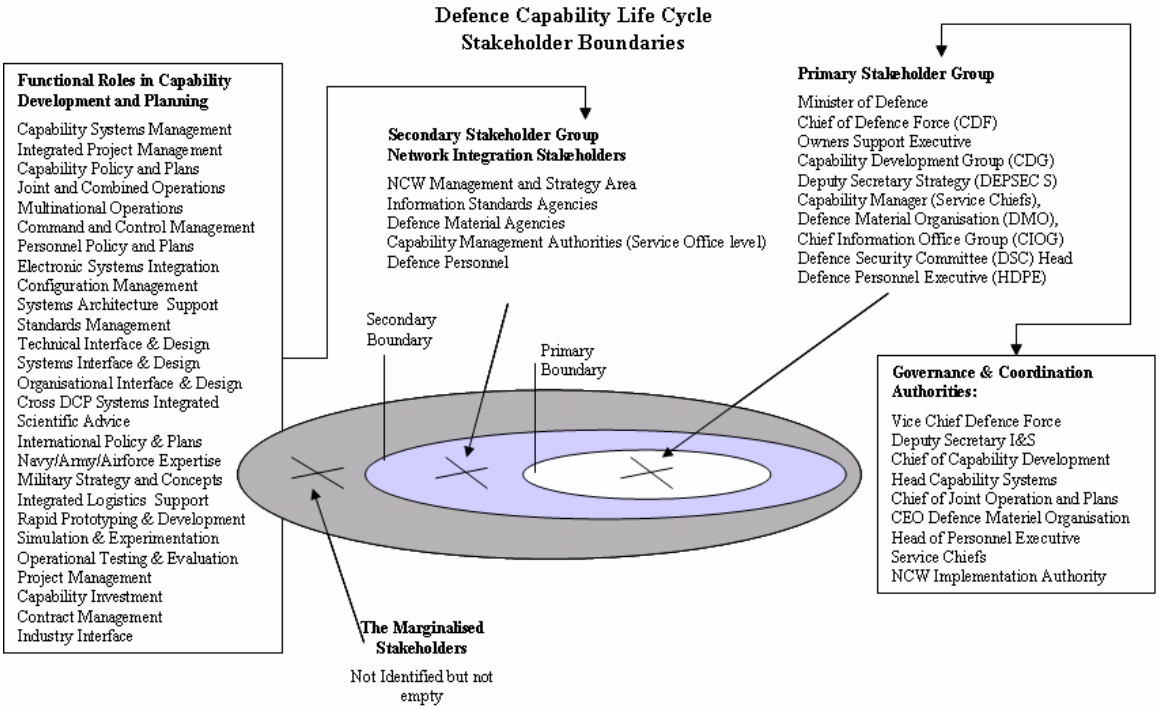

Figure 2 The CD&A stakeholder boundaries based on initial findings June 2005

These stakeholders and functional bodies collaborate at various stages of a projects CLC to support, guide, direct or endorse phases of development, acquisition upgrade or disposal to achieve the desired capability outcome over the of projects lifetime. While the NCW PO will have a key role to play in addressing integration at the project level, the aspiration of developing an integrated NCW capability through the Defence capability process implies significant contributions across Defence.

Key Stakeholder in the NCW CD&A Process

The critical CD&A lead agencies in the primary stakeholder group detailed at figure 2, for coordinating timely inputs from Defence and industry include:

- the CDG for management of the DCP, development projects through to a Government approved solution and oversight of projects in acquisition phase through to Final Operational Capability and Acceptance into Service;
- the Capability Managers[21] for project management;
- DMO for delivering projects and equip and sustain the ADF; and
- CIOG for the development and management of standards and protocols management framework in support of the DIE and DII.

Roles and Responsibilities

To achieve any level of CD&A integration as envisaged with a NCW compliance process which is continuous, with information being fed both into and drawing upon all parts of the CLC process, there are some key activities that need to be conducted. These have been grouped into the following broad areas:

1. Existing CLC activities *as outlined under contextualising the problem space.*
2. The development and integration of a compliance and assessment framework *to be discussed in the section on the* NCW Risk Mitigation Review Framework
3. Activities to support such a NCW framework and process *to be discussed in the* Implementation progress *section*
4. Overarching policy and plan to support the framework and inform CD&A *as initially being addressed by the DCMD 2006 and DCP Integration Plan.*
5. The development of NCW architectural elements and policy *as being coordinated separately under the NCWIT.*

NCW Integration Roles

As indicated in the initial boundary critique results, the introduction of a compliance framework into the CD&A necessitates the formalising and establishment of responsible stakeholder agencies. As indicated at Appendix C at the time of this study, Defence were in the process of raising the NCWIT under HCSD to oversee and implemented an NCW Integration regime to support CD&A. As indicated in the study so far significant oversight will be required to ensure the strategies that come out of NCWIT are implemented. Any new integration roles and responsibilities will impact on business units across the CD&A enterprise, which demands an intervention strategy to achieve a cohesive approach to achieve the level of NCW integration across the DCP. To facilitate this further study is required at the higher level of CD&A which will focus on establishing those higher level tools of government.

Supporting Architecture Responsibilities

One method of capturing the integration requirements is through the use of architectural products. NCW compliance is based, in part, upon analysis of architectural products. Therefore, an understanding of architecture roles and responsibilities is required.

[21] As well as the raise, train and sustain in-service capability requirements through the FIC. They include all Service Chiefs; Chief Joint Operations; Chief Information Officer; DEPSEC I&S and DEPSEC CS.

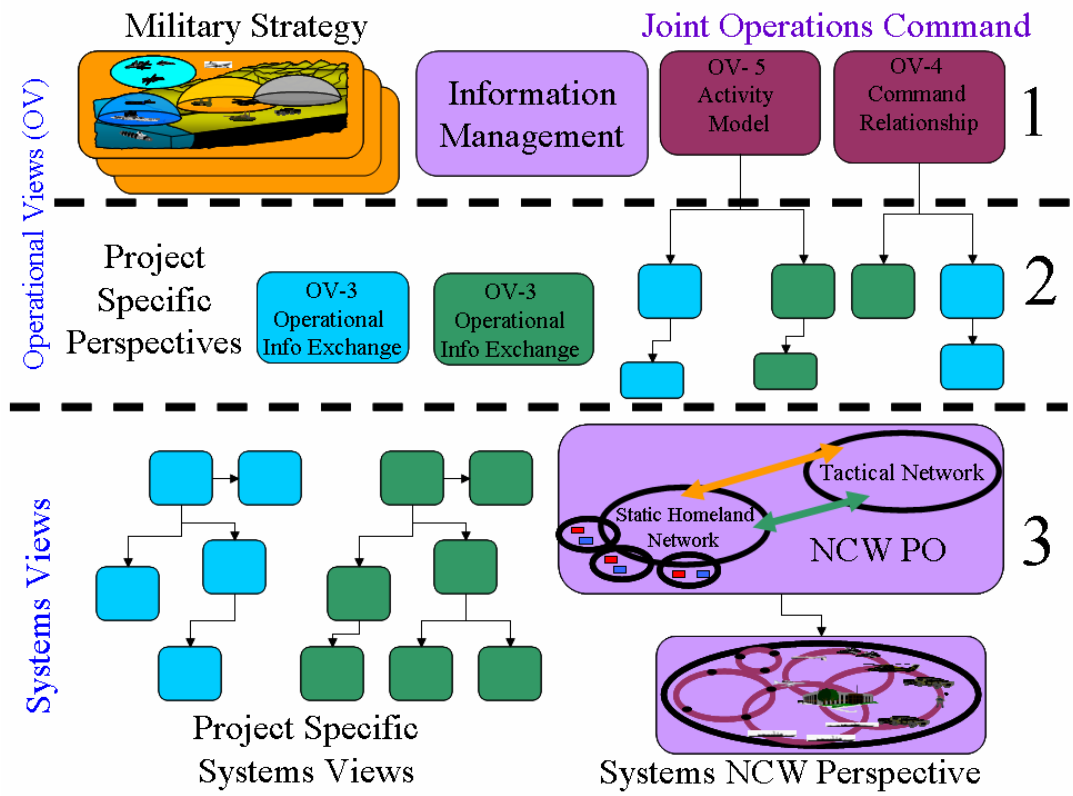

Figure 3 ADF Architecture Deconstruction developed by the SEFFW team.

This is particularly important noting the many stakeholders in CD&A, as detailed previous, involved in the development and evolution of an NCW perspective of the ADO architecture. Figure 3 attempts to identify the principal areas of architectural design and development.

The stakeholders here can be broadly broken into three development groups;

1. *High level Architecture Design.* Those responsible for the architecting the high level concepts. These include the operational views (OV) of OV-1 – the higher level operational concept graphic, OV-5 – the activity model, OV-4 – the command relationship chart and the Information Management policy.
2. *Whole-of-Force Network Centric Design.* Those responsible for architecting the whole-of-force NCW perspective.
3. *Project Architecture Design.* Those responsible for architecting individual capabilities. Capability Managers of projects would produce a sub selection of architecture drawings from on the high level concepts relevant to the whole-of-force perspectives.

Up to now the study has provided an overview of Defence's integration requirements, contextualised the problem space and with the help of enterprise and systems methods highlighted some key issues with the existing CD&A process and captured those considerations for introducing a compliance framework. Systems methods were used on existing policy and guidelines to verify potential stakeholders and areas of responsibility including the development of architectures for supporting the NCW integrated approach to CD&A and the introduction of an NCW compliance process for DCP *Network-centric* capabilities. However, as yet the study has not addressed the types of compliance frameworks and evaluation methodologies

needed to support NCW Compliance. This area is covered in detail in the next section of this paper.

NCW Risk Mitigation Review Framework

During the later period of 2005, following initial trails of the draft frameworks, the team's focus shifted from compliance to risk assessment and risk mitigation. This approach reflects more accurately what could be achieved in assessing levels of capability integration across DCP projects in the absence of mature NCW strategic level guidance. Additionally, while NCW is still in an evolutionary state in the ADF there are currently multiple views of net-centricity depending on the level of command, the level of warfare, the intended C4ISR model, the number and type of players and the NCW capability being sought. With regard to the latter, currently there is insufficient evidence to determine when it is best to use the different views, or how to move between them e.g. when to favour agility over performance. At one stage, it was envisaged that there would be NCW architectures for various epochs to guide future developments, but much needs to be done before such architectures will deliver the desired NCW solution. This is in part due to the "learn by doing" approach to NCW adopted by the Australian Defence Force (ADF) already mentioned.

Thus, in January 2006 there was a shift in research direction by the Systems Enablers for Future Warfare (SEFFW) team from one of NCW compliance towards a NCW risk assessment and mitigation to support the Program Office's NCW Compliance Assessment capability. Given that the first priority of the NCWPO is to maximise the likelihood that project deliverables will be able to integrate into the ADF and coalition forces in a manner that is consistent with current expectations of NCW, the assessment of compliance is more correctly an assessment of the level of risk of a project not achieving a required level of NCW integration and thus the opportunity to highlight potential risk areas in order for projects to develop appropriate and timely risk mitigation strategies.

That is, a NCW risk assessment and mitigation examines the strategies that the projects have in place or identifies the absence of such strategies to deal with the risk of not being able to integrate in a future NCW force. Here, it was agreed that a lower priority would be placed on consideration of potentially desirable attributes of NCW, such as agility and decentralisation. As such, the SEFFW embarked on recasting from a compliance perspective towards the development of a risk mitigation framework and process to support the NCWPO which is hereby referred to as the NCW Risk Mitigation Review (RMR) Framework which can be broken down into constituent views namely:

1. The NCW RMR Systems view
2. The NCW RMR Process view
3. The NCW RMR Assessment view

These views are discussed in detail in the following three subsections.

NCW RMR Systems View

Each project progresses through the capability systems lifecycle individually. The RMR is designed as a dynamic systems process which reaches across the whole CLC. All projects firstly need to be explored individually as a capability and then secondly as an element of the whole capability system. As each capability project changes in the design and developmental stages their level of risk also changes at unit as well as

collectively at force level. Therefore, to effectively assess NCW risks it is necessary to look both across projects and at individual projects. To achieve this, the RMR process is made up of a two connecting databases. One is the NCW view database which contains information on projects that are developing containing information on dependencies and relationships and also which projects are defining which links and networks. The second database is a calling area for all the decisions that have been made, and who is responsible for various standards and protocols within the ADF.

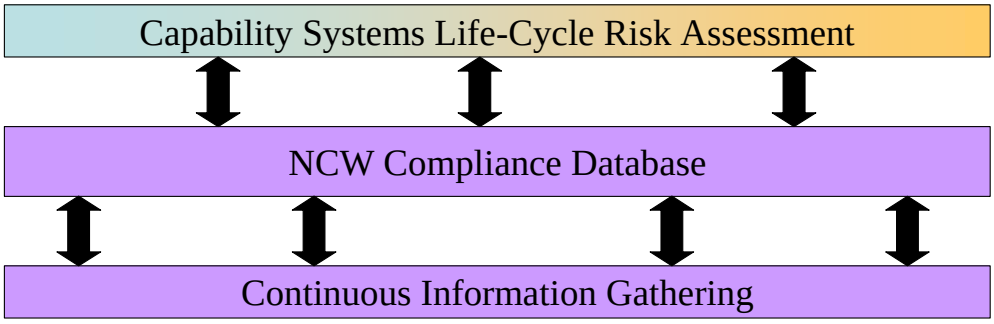

Figure 4 Overall Risk Mitigation Review Systems view

NCW RMR Process View

Although having a continuing process with NCW makes sense there is still a requirement to assist the decision makers and the desk officers producing the project documentation. The NCW Risk Mitigation Review (RMR) process view detailed at figure 4 provides one way NCWPO can manage NCW integration of defence capability through the adoption of NCW Risk Gates. This reduces the risk of delivering a capability that cannot be integrated[22] into the future NCW force, the requirements for integration need to be identified and assessed. Assessment should occur before:

- a decision to expend significant resources on the investigation and refinement of capability options,
- a decision is made by Defence and Cabinet on the preferred solution for acquisition[23], and
- a decision is made to accept the capability for entry into service.

To achieve this, there are three check points integrated into the CLC, one for each of the decision/sign-off points positioned throughout the Defence Capability Systems Lifecycle. Prior to 1st Pass[24] an Initial NCW Risk Review and sign-of is undertaken, and recommendations forwarded for committee endorsement. A similar process is followed at 1st and 2nd Risk Gates with the latter forming part of the Defence Materiel Organisation (DMO) and Capability Manager's Operational Test and Evaluation (OT&E) and Operational Acceptance Trials. These are indicated by the diamonds in Figure 5 below.

---

[22] The reasons for integrating Defence capabilities are discussed in more detail in the next section.

[23] It is recognised that the tender process might have commenced at this stage, however Program Office interactions between risk gates should be sufficient to ensure that any deficiencies can be rectified during contract negotiations.

[24] At 1st Pass capability projects must present to Government alternatives to meeting an agreed capability gap in the form of an endorsed capability proposal first pass (CPFP) documentation package. This provides Government the opportunity to narrow the alternatives being examined. Approval to proceed at this stage is approval to further develop selected options/alternatives and is also endorsement to include the project in the DCP and the Major Capital Investment Program.

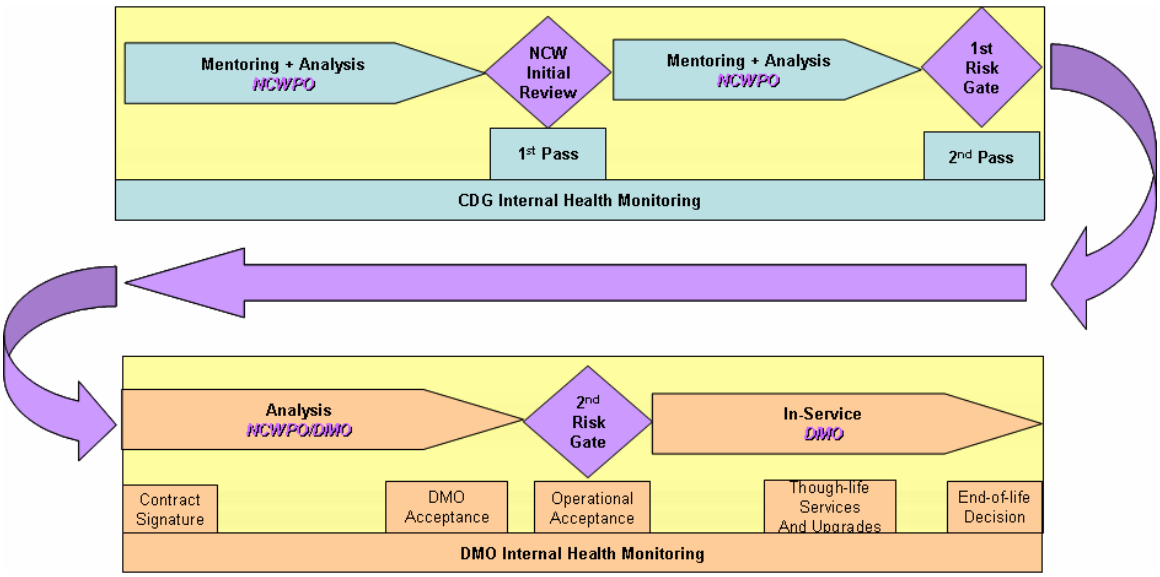

Figure 5 NCW Risk Mitigation Review Process View

NCW RMR Assessment View

To address the NCW issues identified earlier theoretical studies were conducted to design and develop an appropriate assessment framework to support the NCW RMR Framework. This work is the subject of the second paper being presented at this symposium, however, what follows is a brief outline of the assessment view developed as part of this activity.

The Risk Mitigation Review model comprises of four analysis areas shown at figure 6, which are drawn upon depending on the *capability lifecycle stage* the project is entering at the time e.g. *requirements, acquisition in-service and disposal.*

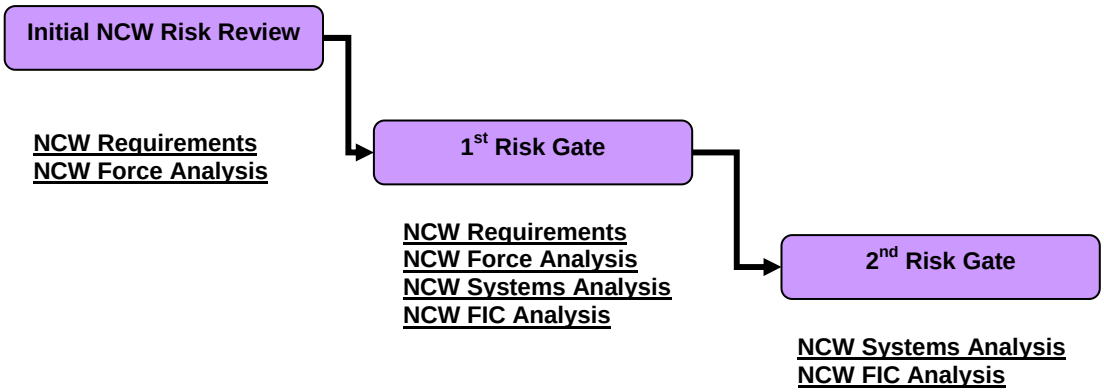

Figure 6 NCW Assessment Gates.

These analysis areas are detailed as follows:

NCW Requirements Analysis This area explores the high level context for the capability. It analyses the justification for the NCW-related requirements, including the NCW effects to be delivered, the NCW characteristics of the project and the relationships required with other capabilities.

NCW Force Analysis This area is focused on assessment of the project in the context of the Capability Life Cycle (CLC) and the Defence Capability Plan (DCP), and covers issues such as how the capability options fits with other capability (options) decisions on scheduling, resources, and revising the DCP.

NCW Systems Analysis This area explores in more detail the requirements placed either on the capability by outside capabilities that are in service, under development or planned and vice versa.

NCW FIC Analysis This analysis area explores if there are any *fundamental input to capability* issues with the introduction of the capability and its NCW elements. This could include training to exploit new NCW elements and the processes, doctrine etc that result.

Each *NCW Analysis Area* is comprised of a select number of *Criteria* which are divided into *Categories* with *Questions Lists* which are applied by the CDG NCW Assessment Team to Capability Projects transitioning through the CD&A phases. Appendix E provides a table which details the four analysis areas of the framework and supporting criteria as at January 2006.

Implementation progress

The following section provides a summary of progress to date.

NCW Compliance Development

CDG have made significant progress towards the integration of an NCW compliance process into the Defence CLC. The NCW-RMR framework described in the previous section underpins the *NCW Compliance Process*, which is now contained in the Defence Capability Development Manual - *Blue Book* (DoD 2006). Meanwhile, development continues on refining the NCW RMR. The overall NCW assessment capability being raised in CDG is now referred to as the NCW Capability Assessment Process (NCAP). It is expected that this process will continue to explore and draw upon a number of assessment methods including RMR which are either under development nationally or in use internationally over the next few years in order to formalise a compliance package/ toolbox of methods to cover the broad range of compliance issues.

Development of the NCW RMR Training Package

This study team have developed a training package based on trials of the framework to support the induction the CDG NCW Compliance Assessment Cell and projects teams into NCW compliance framework and assessment process.

NCW Capability Assessment Process (NCAP) Prototype.

An NCAP tool prototype was designed and developed by the study team to show the CDG NCWPO how a tool could help them in managing the assessments of various projects i.e. it was intended as a concept demonstrator not a working tool. The fact that the NCW Assessment Cell are able to use the prototype has been a bonus for CDG until such time that a more comprehensive and robust capability can be raised and incorporated into the capability development database.

NCW RMR Framework Handover

As this study is due to be finalised in June 2006, the team are in the process of finalising research for handover to the NCWPO before the termination date.

Conclusion

This paper describes the initial research conducted by SEFFW to design and develop an overarching NCW RMR framework in support of the ADF's requirement for an integrated Defence Capability Plan. This research employed various systems tools to provide a foundation for Part *Two* by describing the CD&A program in the context of the NCW compliance requirements. The paper reviews the CD&A process, CD&A as an enterprise (in a dynamic socio-economic and information-technology environment), identifies the various stakeholders boundaries and describes problem areas for NCW acquisition before outlining a NCW RMR framework for the capability planning process to ensure compliance of projects throughout their CLC.

From concept to capability NCW is still in an evolutionary state and much needs to be done before a suitable architecture and standards capability are available to inform CD&A forecasting. The RMR framework, attempts to address NCW compliance from a more generic risk perspective *i.e. what is the level of risk of a project not achieving a required level of NCW integration,* Research continues with the development of the RMR framework to support the client. It is expected NCW compliance as still a relatively immature capability will continue to explore and draw upon a number of assessment methods including RMR over the next few years to establish a toolbox of methods to cover the broad range of compliance issues.

Appendices

A. MIT90 Enterprise Model in the CD&A NCW Problem Space
B. Applying Total Systems Intervention (TSI) Process
C. Critical Systems Heuristics and the Boundary Critique Methods Employed
D. Critical System Heuristics & Boundary Results
E. NCW Risk Mitigation Review Framework
F. Acronyms

References

Alberts, D. (2003). *Power to the Edge: Command and Control in the Information Age,* Command and Control Research Program Publication Series, ISBN 1-893723-13-5.

Borgu, A. (2003). The Challenges and limitations of Network Centric Warfare - The initial views of an NCW sceptic. Network Centric Warfare Conference, Canberra.

Cook, S. (2000). Assessing the C4ISR Architecture Framework for the Military Enterprise. University of South Australia, Systems Engineering and Evaluation Centre.

Dekker, A. (2006). "Measuring the Agility of Networked Military Forces." *The Journal of Battlefield Technology* **9**(1): 19-24.

DoD (2002). *Defence Information Environment Architecture Principles,* Department of Defence.

DoD (2002). *Future Warfighting Concept,* Canberra, Defence Publishing.

DoD (2003). *Defence Procurement Review 2003*, Canberra, Department of Defence.

DoD (2004). *Enabling Future Warfighting: Network Centric Warfare*. Canberra, Defence Publishing Service.

DoD (2005). *The ADF Network Centric Warfare Roadmap,* Canberra, Department of Defence.

DoD (2006). *Defence Capability Development Manual*, Canberra, Department of Defence.

Flood, R. and M. Jackson (2002). *Creative Problem Solving.* West Sussex, Wiley and Sons.

Flood, R. and M. Jackson (1991). "Total Systems Intervention: A Practical Face to Critical Systems Thinking." *Systems Practice* **4**(3): 197-213.

Kaufman, A. (2004). *Curbing Innovation: How Command Technology Limits Network Centric Warfare.* Canberra, Argos Press.

Kingston, G., W. Richer, et al. (2006). NCW Risk Assessment Theory. 11th International Command and Control Research and Technology Symposium.

Midgley, G., I. Munlo, et al. (1998). "The Theory and Practice Of Boundary Critique." *Journal of the Operational Research Society*.

Perry, W., W. Button, et al. (2002). *Measures of Effectiveness for the Information-Age* Navy. Santa Monica, RAND.

Scholz, J. and D. Lambert (2005). A Dialectic for Network Centric Warfare. 10th International Command and Control Research and Technology Symposium.

Scott Morton, M. S. (1991). *The Corporation of the 1990s, Information Technology and Organisational Transformation.* New York, Oxford University Press.

Shekmar, S. and J. Kreger (2004). *US Net-Centric Checklist*, Office of Force Transformation.

Ulrich, W. (1987). "Critical Heuristics of Social Systems Design." *European Journal of Operational Research.*

US DoD (1997). *C4ISR Architecture Framework,* Version 2.0, US Department of Defence.

Warne, L., A. Irena, et al. (2004). The Future Warrior. 9th International Command and Control Research and Technology Symposium.

Appendix A: MIT90 Enterprise Model in the CD&A NCW Problem Space

MIT90 NCW Framework

As described in the main paper, the MIT90 framework describes an information-technology (IT) enabled organization which comprises five interacting "forces" namely *technology, individuals and roles, structure, management processes and strategy* that respond individually and collectively to those external environmental pressures as shown in figure A1 below.

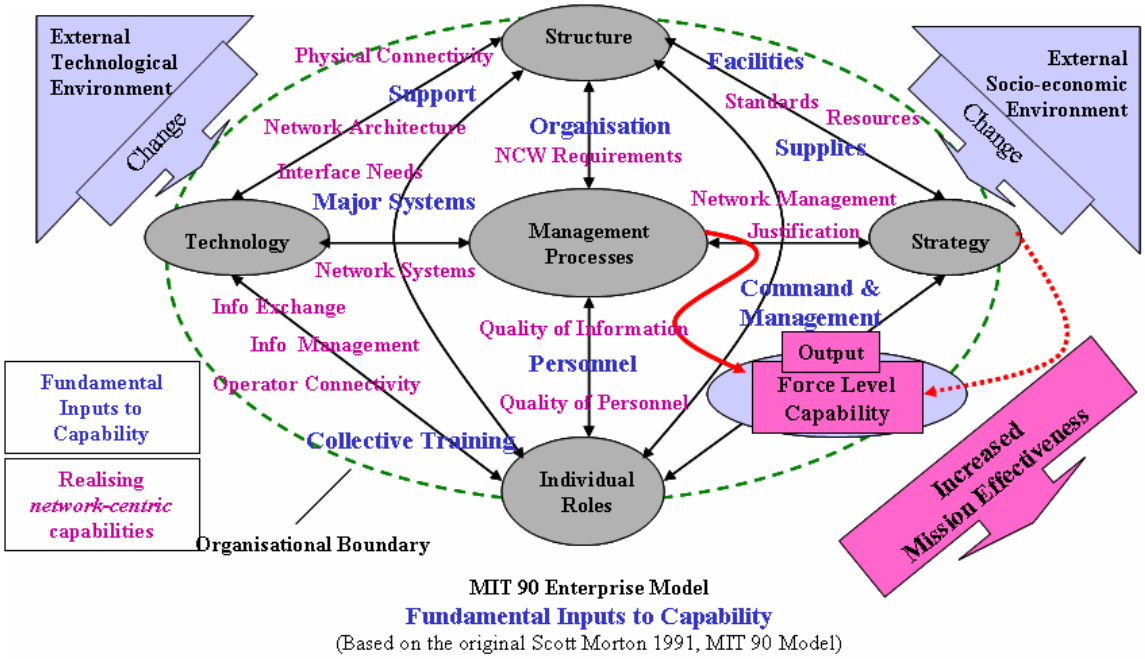

Figure A1.The MIT 90 Model overlaid with the components of the FIC (blue) and the capability inputs for achieving an integrated NCW approach (purple) to CD&A and a systems of systems approach to Force Level Capability.

As detailed in Figure A1, the original MIT90 model has been adapted to suit the CD&A *network-centric* integration problem space. This has been achieved by firstly superimposing over the model the ADF Fundamental Inputs to Capability (FIC) elements and later during the development stages, building in those perceived *network-centric* capability inputs drawn from the 2004 *NCW Roadmap's* fundamental NCW elements of *network, networking and the human dimension.* This revised NCW model of MIT90 provided some members of the team with a reference point from which to progress as well as constant reminder and appreciation of the breadth of NCW issues which in many ways impact on the model's five forces.

MIT 90 NCW High Level Questions List

Employing this revised framework during the study provided a foundation from which to move forward. As discussed in the paper, the following were the initial questions raised during the review of literature and client discussions. These have been categorised according to the revised MIT90 five forces as follows:

Strategy
What are the strategic risks involved?
What is the *NCW Integration plan*?
What are the lines of reporting and responsibility for NCW integration?
What does a *NCW Compliance* framework look like?
How do we *justify* the increased cost for introducing *NCW capability* in projects?

Management Processes
What are the management and process risks involved?
What is the *NCW Compliance* impact on organisational distribution of power and control?
Who has overall responsible for *NCW Compliance* of future capability?
Who are the responsible agents for NCW *Compliance* assessment sign-off?
What does it mean to be *NCW* compliant anyway?
What are *NCW Compliance* levels of risk/confidence?
From a CLC perspective where should *NCW Compliance Checks* be positioned?
Do all projects have to attain the same level of compliance?
Do all projects have to be compliant?

Structure
What are the *organisational structural* risks involved?
What is the structure of an *NCW compliant* capability?
Who are the *key stakeholders* of the *NCW compliant* capability?
What are their responsibilities?
Who are the affected agents of an *NCW compliant* capability?
What are the *NCW core and supporting* projects to achieving a *force 2020* target?

Individual Roles
What are the *human-dimensional* risks involved?
What are the likely *cultural* issues *Compliance assessment* will have to address?
What are the likely *ethical* issues with *NCW Compliance monitoring & assessment*?
How do you manage and promote *trust* in a *NCW Compliance environment*?
What changes will *NCW Compliance* make to assigned roles?
What is the *human-dimensional* impact of adopting an integrated approach to NCW?
Who is addressing this area?
What are *NCW Compliance* implications for training and education?

Technology
What are the *technical risks* involved?
How will *technical risks* be prioritised?
What impact will they have on the projects status?
How do we ensure integration at the *network* and *systems level*?
What are *NCW interface dependencies*?
What are *core NCW projects*?

What are *supporting NCW projects*?
What are the *interoperability* and *connectedness* issues with *NCW Compliance*?
What capabilities will be *reliant* on core and supporting technologies?

Appendix B: Applying Total Systems Intervention (TSI) Process

Total Systems Intervention (TSI) Process

Total Systems Intervention (TSI) (Flood and Jackson, 2002) employs three phases, as described at table B1, which are designed to support selection of suitable interventions that can be applied to an organisation's problem space providing a creative systems thinking approach to informing organisational change.

TSI Phases	Description
Creativity	
Task	To highlight aims, concerns and problems.
Tools	Systems metaphors.
Outcome	*Dominant* and *dependent metaphors* highlighting the major issues.
Choice	
Task	To choose appropriate systems-based intervention methodologies.
Tools	The "system of systems methodologies"; the relationship between metaphors and methodologies.
Outcome	*Dominant* and *dependent methodologies* chosen for use.
Implementation	
Task	To arrive at and implement specific change proposals.
Tools	Systems methodologies employed according to the logic of TSI.
Outcome	Highly relevant and co-ordinated intervention.

Table B1. The TSI methodology, an extract from Flood and Jackson, 2002 p54.

To identify appropriate *interventions* is dependant on the *problem context.* Determining the *problem context* is dependent on identifying the *dominant and dependent metaphors.* These metaphors are linked to *systems of systems methodologies* (SSM) framework which categorises these metaphors according to *problem context. The problem context* in turn assists in determining appropriate methodologies for the contingent tasks. The following describes the two phases of TSI which captures this process.

Creativity - Grouping by Metaphors

To assist in the filtering when analysing the problem context TSI employs *systemic metaphors* as the lens through which to describe an organisation based on the complex interactions observed. They are:

- *machine* metaphor, or closed systems view
- organic metaphor (*organism*) or open systems view
- neuro cybernetic (*brain*) metaphor or variable systems view
- *cultural* metaphor
- political (*team, coalition and prison*) metaphor

Choice - Grouping by Problem Context

According to Flood and Jackson (2002, p51), *methodologies* can be categorised according to *problem context*. The two context dimensions used here are: One by *system type,* and Two by *participant relationship* with other players.

One. System types are categorised as:

- *simple systems* - 'closed systems' which are small or highly organised with few interactions or
- *complex systems* – 'open systems,' principally large, consisting of many elements, with many interactions, purposeful, and probabilistic in their behaviour and evolving over time.

Two. Participant relationships are categorised as either:

- *unitary relationships*, where they share common interests, value, beliefs, are participative, agreeing upon common ends and means, or
- *pluralist relationships* where beliefs, though compatible, diverge, but area amenable to compromise in decision making or
- *coercive relationships* which do not share common goals, where values and beliefs are most likely in conflict, there is no agreement on objectives and a tendency to coerce others in decision making.

	Unitary	**Pluralist**	**Coercive**
Simple	**Simple Unitary** The organisation as a: • *machine* or *team* (closed systems view)	**Simple Pluralist** The organisation as a: • *culture* and *coalition* (political)	**Simple Coercive** The organisation as • *a prison* (political)
Complex	**Complex Unitary** The organisation as a: • *organism* (organic) and *brain* (neuro-cybernetic)	**Complex Pluralist** The organisation as a: • *culture* and *coalition* (political) as well as the *organism* and *brain*	**Complex Coercive** The organisation as • *a prison* (political)

Table B2. The association between problem context and metaphors adapted from Flood and Jackson (2002, p35-51) .

Table B2, captures the relationship described between the *categories of problem context* and the *metaphors* thereby assisting in the identification of appropriate *interventions* at Table B3, based on the *dominant metaphor* of the organisation. The following details the approach taken early in the task to better understand the *problem space* and to support this area of research.

	Unitary	Pluralist	Coercive
Simple	**Simple Unitary** *Methodologies:* • Operational Research • Systems Analysis • Systems Engineering • Systems Dynamics	**Simple Pluralist** *Methodologies:* • Social Systems Design • Strategic Assumption Surfacing and Testing	**Simple Coercive** *Methodologies:* • Critical Systems Heuristics
Complex	**Complex Unitary** *Methodologies:* • Viable Systems Diagnosis • General Systems Theory • Socio-technical Systems Thinking • Contingency theory	**Complex Pluralist** *Methodologies:* • Interactive Planning • Soft Systems Methodology	**Complex Coercive** *Methodologies:* • Nil

Table B3. Drawn from Flood and Jackson (2002, p43) which assists in the identification of the intervention strategy based on the research assumptions of the problem context.

Applying TSI to the Capability Development & Acquisition Enterprise.

Based on the client briefing received at the outset[25], the supporting papers, follow-up discussions with client staff officers and a review of capability development discussion papers and documentation, the team were able to develop a rich contextualised picture of Capability Development and Acquisition (CD&A) with which to identify the *dominant and/or dependent metaphor(s)*. With this information, the team would then be able to identify suitable systems *intervention methodologies.*

In determining a suitable *intervention methodology* it was argued, based on the data collected, that the enterprise tended to display a *political* systems view. Metaphorically this is a *coalition or prison view* which describes *complex pluralist* to s*imple coercive* problem area as detailed at Table B3. Here the enterprise is viewed as one which is continually influencing, as well as being influenced by, numerous internal and external cross coalition political issues in addition to those external domestic and international issues that arise with respect to a competitive defence industry and finance environments. Further analysis suggested a bias more towards the *prison* rather than the *coalition* as the *dominant metaphor,* as such the *intervention* chosen was the Ulrich (1987), Critical Systems Heuristic (CSH) checklists and Churchman's (1970) Boundary Critique methodology.

Insight to the complexity of CD&A

Within the CD&A enterprise, organisations and their agencies are constantly dealing with many complex and time critical capability life-cycle issues that span across defence, agencies, government and industry both at national as well as international levels. At any time, there is anywhere up to 120 projects, at various stages of approval, transitioning through the DCP process e.g. the proposed future acquisition of three Air Warfare Destroyers, the Joint Command Support System, the Joint Strike Fighter. Many are at various stages of acquisition and acceptance testing e.g. Collins Class submarine and the ANZAC Class Frigate. As the need for a new capability is accepted and it progresses through the capability development and acquisition

[25] This research into stakeholders and responsibilities was conducted during the initial development of the Task Plan between the client and DSTO in the period of May – July 2005.

phases, it draws upon a diverse number of stakeholders and contributors each with many complementary but also differing goals.

To explain, the CD&A enterprise is made up of many cross-organisational business units, which are required to exchange services, monitor or meet various timelines and have responsibilities across Defence and external agencies.. Individual project issues can be diverse, each with competing aims and in other cases dependencies e.g. time sensitive delivery of enabling or supporting capabilities. As such members come to the table with underlying project level *platform-centric* views yet seeking approval for a force level *capability-centric* system. To support CD&A management, the enterprise employs project management-style tools and processes through a capability maturity framework more suggestive of a *hard systems* approach along *systems engineering* lines.

The requirement to establish and overlay an NCW compliance framework on the existing DCP process and identify appropriate responsible stakeholders likewise is subject to the internal politics between major stakeholders during these design, development and implementation stages.

The problem is also one of boundaries; that is, who are prime stakeholders, who are the supporting or secondary stakeholders, who are the decision makers within these boundaries, and of these, who are necessary to support the introduction and maintenance of an NCW compliance process. Establishing boundaries requires a great deal of knowledge of the system and players, including their levels of responsibility and degree of involvement during the capability development and acquisition phases as well as in-service and disposal, a period which could be as long as 7-10 years for technical systems and 25 years including significant upgrades for major capability systems. To support this level of research Ulrich's (1987) critical systems heuristics checklist (see appendix C) was used to better display the whole CD&A problem space in a tabulated form (based on the data collected) in order to display all stakeholders. This information was then feed into Churchman's (1970) boundary critique method (see appendix D) which provides an overview of stakeholders in the form of an easily recognisable rich picture.

Appendix C: Critical Systems Heuristics and the Boundary Critique Methods Employed

The Critical Systems Heuristics (CSH) checklist was applied to the data collected as discussed at Appendix B to identify in a more easily examined tabulated form all stakeholders in the Defence Capability Development & Acquisition (CD&A) enterprise. The Boundary Critique Method was used to just support the identification of boundaries of influence, decision making power and responsibilities from concept to the delivery of capability. The intent here being that the information would be used to support ongoing discussions with the client, stakeholders and interested parties. The following provides an overview of the CSH and Boundary Critique methods.

Applying the Critical Systems Heuristics Checklist

Ulrich (Flood and Jackson 2002) and (Midgley, Munlo et al. 1998), produced a checklist of twelve boundary questions to determine those involved and those affected. The checklist is organised into four groups of boundary judgements each containing three categories. Instantiations of these checklist questions were used in the study as described in tables C1 & C2 below. The four groups are as follows: the *client* - the source of **motivation**, the *decision maker* - the source of **control**, the *designer* - the source of **expertise**, and the *witness* - reflecting the source of **legitimation**.

The Critical Systems Heuristics (CSH) Checklist

As guided by (Ulrich 1987) methodology, the twelve CSH checklist of questions have been substantiated with respect to the problem space in question namely:

- What currently *is* the case in Capability Development & Acquisition or the Defence Capability Planning (DCP) Process?*(see Table C1)*
- What *ought* to be the case in Capability Development & Acquisition incorporating an NCW Compliance Framework?*(see Table C2*

	Nº	Critically Heuristic Boundary Questions
Motivation	1	Who *is* the actual **beneficiary** of the DCP Process design, i.e. who belongs to the group of those whose purpose (interest and values) are served?
	2	What *is* the actual **purpose** of DCP Process design, as being measured not in terms of declared intentions of the involved but in terms of the actual consequences?
	3	What, judged by the design's consequences, *is* its built in **measure of success**?
Control	4	Who can actually change the measure of success? Who *are* actually the **decision makers?**
	5	What *conditions* of successful planning and implementation of the DCP Process are really controlled by the **decision makers?**
	6	What *conditions* of the DCP Process *are* not controlled by the **decision makers**, i.e. what represents **environment** to him?
Expertise	7	Who *is* actually involved as **designer in the** DCP Process?
	8	Who *is* involved as the **expertise** of the DCP Process (and roles played and expertise type)?
	9	a. Where do the *involved* see the **guarantee** that their planning will be successful? b. Can these assumed **guarantees** secure the design's success, or are they false guarantors?
Legitimacy	10	a. Who among the involved agencies (**witnesses)** to the DCP Process *represents* the concerns of the affected? b. Who *is* or may be *affected* without being involved?
	11	Are the affected given an opportunity to **emancipate** themselves from the experts and to take their fate intro their own hands, or do the experts determine what *is* right for them, what quality of life means to them, etc? (That is to say, are the affected used merely as means for the purpose of others, or are they also treated as "ends in themselves," as belonging to the client?)
	12	What **world-views** *is* actually underlying the design of the DCP Process? *Is* it the world view of (some of) the involved or of (some of) the affected?

Table C1. The 12 critically heuristic boundary questions in the "is" mode.

	Nº	Critically Heuristic Boundary Questions
Motivation	1	Who *ought* to be the **beneficiary** of the CD&A Process (incorporating an NCW Compliance framework)?
	2	What ought to be the **purpose** of the CD&A Process, i.e., what goal states ought S be able to achieve so as to serve the client?
	3	What *ought* to be the CD&A **measure of success**?
Control	4	Who *ought* to be the **decision makers**, who have the power to change the CD&A Process **measure of improvement**?
	5	What **components** (resources and constraints) of the CD&A Process *ought* to be controlled by the **decision makers?**
	6	What resources and conditions (should be **environmental***) ought* not be controlled by the CD&A **decision makers?**
Expertise	7	Who *ought* to be involved in the **design** of the CD&A Process?
	8	Who *ought* to be considered an **expert** and what should be their role in the CD&A Process?
	9	What *ought* to be the **guarantees** of the CD&A Process, i.e., judged by the CD&A measure of success?
Legitimacy	10	What agencies or position *ought* to belong to the **witnesses** representing the concerns of the Services that will be affected by the design of the CD&A Process i.e. who among the affected *ought* to get involved?
	11	To what degree and in what way *ought* the affected be given the chance of **emancipation** from the premises and promises of the involved?
	12	Upon what **world-views** of either the involved or the affected *ought* the CD&A Process design be based?

Table C2. The 12 critical heuristic boundary questions in the "ought" mode.

Appendix D provides an example of the application of the CSH methodology to the problem context to provide a higher level view of those clients, decision makers, designers and users (witnesses) and their individual and collective responsibilities in the current CD&A processes and with the incorporation of NCW compliance gates into the capability life of type management.

Applying the Boundary Critique Method

Churchman (1970) recognised that boundary judgements are intimately linked to *value judgements*. As sighted in Ragsdell, (2001), Ulrich (Ulrich 1987) argues that rather than values, the determination of boundaries should be a *rational process* based on dialogue of those groups, organisations, etc… who will be involved and or affected by the intervention. An example of the boundary judgement concept is displayed in Figure C1. It details the primary and secondary boundaries and the marginalised area, the potential source of conflict, which lies in-between such boundary lines. When such boundary judgements exist, it gives rise to ethical dilemmas that need to be resolved in order to move forward with the intervention. Likewise *critical system thinking* without system boundaries would be subject to boundary creep and loss of strategic focus. (Midgley, Munlo et al. 1998) on consideration of both Churchman's and Ulrich's approaches ask the question, *what happens when there are conflicts between different stakeholders making different value and boundary judgements?*

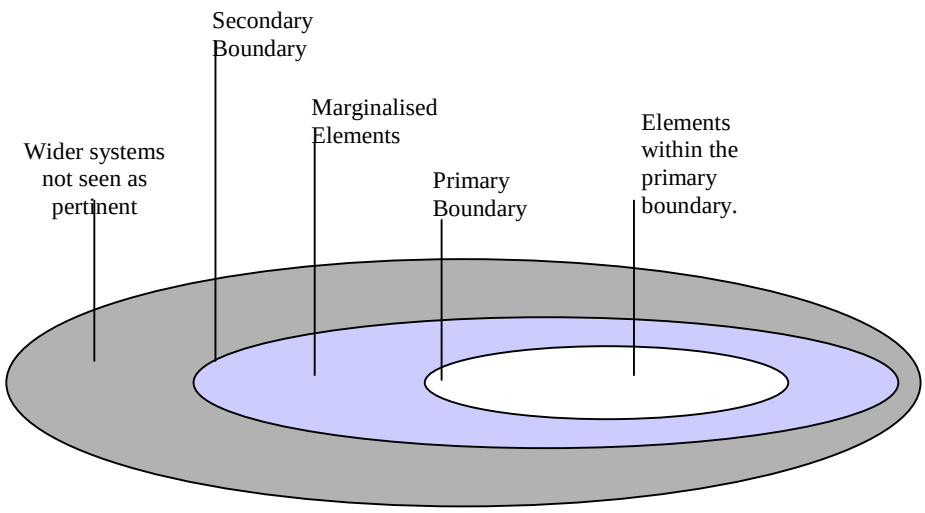

Figure C1. Primary and Secondary Boundary Judgements and Marginalisation.

Critical systems thinking is intimately linked to boundary judgements through the boundary critique process. Midgley's approach is to declare such *ethically marginal areas* as either *sacred* (*valued* – of special importance) or *profane* (*devalued* – can be dismissed) as shown in figure C2. Overlaying such *ethical* issues are the *symbolic expression in ritual*[26]. Consideration of these overlaying *rituals* in the first instance is a

[26] Where one ethic arises within the primary boundary, and another arises in the secondary boundary they will come into conflict and can only be dealt with by making elements in the boundary margin either *sacred* or *profane*. This is referred to as *symbolic expression in ritual* and here is a rather

good indicator of just where *value or devalued elements* lie and where ethical conflicts can be found in the area of *marginalisation*. Results of this method applied to the CD&A environment is detailed at Appendix D.

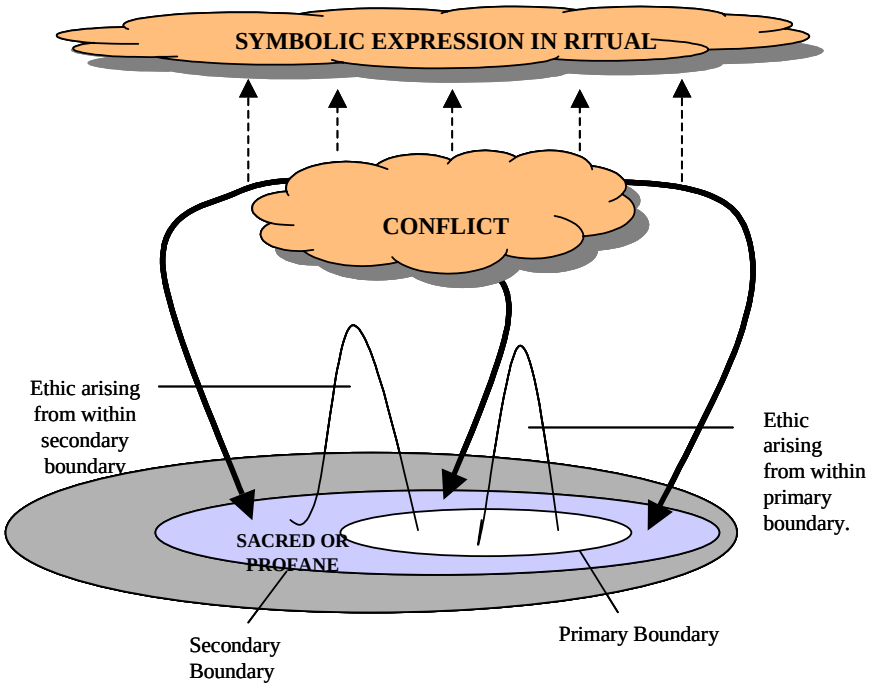

Figure C2. Resolving Marginalisation issues between Boundary Judgements.

simplistic description of an otherwise complex issue which is discussed further in Midgley, (Midgley, Munlo et al. 1998) .

Appendix D: CSH & Boundary Results

The initial results of the Boundary Critique Method based of the findings from the CSH spreadsheets are captured diagrammatically in the following boundary diagrams as follows.

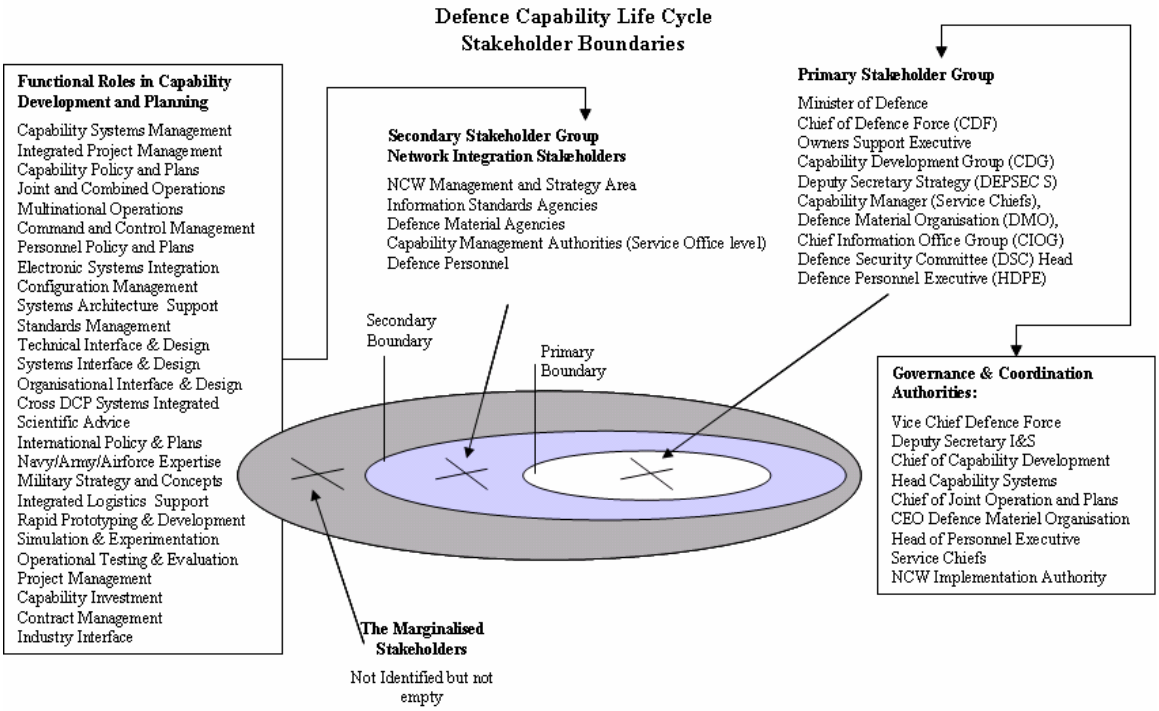

Figure D1. This is a rough cut of stakeholder boundaries based on initial findings.

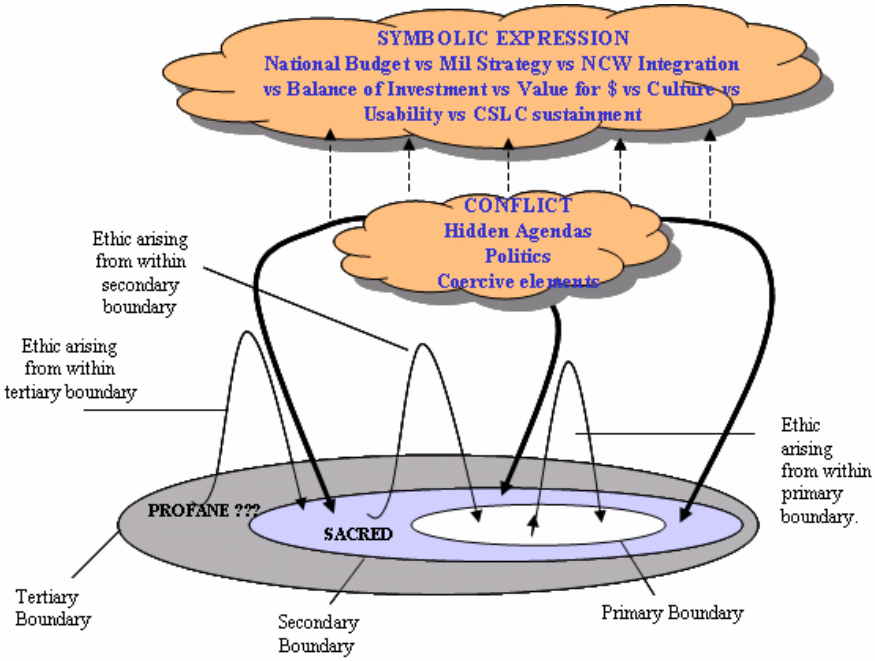

Figure D2. An appreciation of the areas of conflict and political issues in such a diverse cross enterprise membership.

Appendix E: NCW Risk Mitigation Review Framework

The following tables describe the criteria underpinning the NCW RMR analysis framework.

Area	Criteria	Description
NCW Requirements Analysis	Background	This criterion determines if an NCW Assessment is necessary and if so, to capture information about the project that can be used in its analysis and the analysis of other projects.
	Justification	This criterion examines the justification for the project and its interfaces, as well as the consistency and completeness of the interfaces.[27]
	Justifications – Options Implications	This is a subset of justification which looks at the implications each option has on the delivery of the expected NCW capability and whether they are supported by comparative studies.
NCW Force Analysis	Interaction Responsibilities	This criterion which assesses how responsibilities for providing the interface have been divided. It covers whether or not responsibility for ensuring interoperability has been identified. This includes identifying the requirements, and responsibility, for establishing gateways.
	Resources Allocation	This criterion assesses the suitability of available personnel and financial resources to deliver the required NCW capability. It covers the degree to which physical and communications requirements have been identified and resourced for each option.
	Resource Allocation – Options Interfaces	This is a subset of resources allocation which looks at the resource necessary to support the interfaces of each option. This includes requirements for development, delivery implementation and sustainment of interfaces for networks including gateways the project will provide and the standards and protocols employed.
	Timelines	This criterion assesses whether infrastructure projects will be delivered before those that will rely upon them. It covers whether or not dependencies between projects are consistent with their delivery timelines.

Table E1 NCW Risk Mitigation Review Framework covering NRA and NFA Areas completed.

[27] Assessing this criterion involves consideration of the justification for the project and the interfaces, and their completeness and consistency of the interfaces. The objective is to ensure that the project will deliver: the required NCW capability, the interfaces required by other capabilities, and ensure other projects will deliver the capability required by the project being assessed.

Area	Criteria	Description
NCW System Analysis	Standards Responsibilities	This criterion is concerned with the responsibilities for ensuring alignment of the Project and options to those new and existing Standards and Protocols which will affect it over the CLC. It consists of a series of questions to identify responsibilities for the provision of new standards and protocols proposed for use in the available documentation.
	Operator Connectivity	This criterion covers the human elements in the system and whether operators are able to perform their required roles. It covers whether the capability options will facilitate or hinder operator interactions.
	Applications Management	This criterion covers whether or not the appropriate applications have been identified and their ability to interpret data in a consistent and appropriate manner. This criterion is intended to combine the ISO models applications and presentations categories.
	Information Management	This criterion covers what information is exchanged, whether or not the information management procedures of the capability options are identified and consistent with those of related capabilities i.e. how it is exchanged (including management of information flow, data transfer, assurance and fusion).
	Physical and Communications Connectivity	This criterion combines the ISO models physical and data link categories, it covers the degree to which physical and communications (including consideration of spectrum, integration, bearers, standards, protocols and others) requirements have been identified.
	Network Management	This criterion covers whether or not network management (including management of traffic flow, connectivity, bandwidth, spectrum, emissions and gateways) of the capability options are identified and consistent with those of related capabilities.
NCW FIC Analysis	Australian FIC	*Here it is intended using other methodologies being developed concurrently to this study for NCWPO*, to employ the current Australian FIC categories which include: organisation, personnel, collective training, major systems, supplies, facilities, support and command management. These criteria will examine whether or not FIC elements are appropriately addressed, resources, and commonalities identified.

Table E2. NCW Risk Mitigation Review Framework covering NSA and NFIC Areas completed.

Appendix F: Acronyms

ADDP	Australian Defence Doctrine Publication
ADF	Australian Defence Force
ADO	Australian Defence Organisation
C4ISRAF	C4ISR Architecture Framework
CCDG	Chief CDG
CD&A	Capability Development & Acquisition
CD&E	Concept Development & Experimentation
CDG	Capability Development Group
CIO	Chief Information Officer
CIOG	Chief Information Officer Group
CLC	Capability Life Cycle
CSD	Capability Systems Division
CSH	Critical Systems Heuristic
DCDM	Defence Capability Development Manual
DCP	Defence Capability Plan
DCS	Defence Capability Strategy
DGICD	Director General ICD
DID	Defence Information Domain
DIE	Defence Information Environment
DII	Defence Information Infrastructure
DMO	Defence Materiel Organisation
DNCWI	Director of NCW Implementation
DOD	Department of Defence
DSAD	Defence Systems Analysis Division
DSTO	Defence Science and Technology Organisation
FIC	Fundamental Inputs to Capability
FOC	Final operational Capability
HCS	Head Capability Systems
ICD	Integrated Capability Division
LOT	Life of type
MIT90	Management in the Nineties
NCW	Network Centric Warfare
NCWI	Implementation
NCWIT	NCW Implementation Team
NCWPO	NWC Program Office
OT&E	Operational Test and Evaluation
OV	Operational Views
RD	Rapid Development
RMR	Risk Mitigation Review
RPDE	Rapid Prototype Development and Evaluation
SEFFW	Systems Enablers for Future Warfare
SSM	System-of-Systems Methodology
TSI	Total Systems Intervention