Assigned Number: I-111

11TH ICCRTS

COALITION COMMAND AND CONTROL IN THE NETWORKED ERA

Title: NCW Risk Assessment Theory

Topics: Policy, C2 Architecture, Network Centric Metrics, C2 Analysis

Gina Kingston, Warren Richer, Elizabeth Kohn

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 Theory and Philosophy

Abstract

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). This document is the second of two being presented to this 11th ICCRTS and describes the theory and philosophy behind that framework. The companion paper, NCW Risk Assessment Policy and Process (Richer et al. 2006) describes the stakeholder and proposed overarching RMR framework developed in support of the client.

During this research activity the authors became aware of existing leading compliance models and some of these models—many developmental—that focus on specific warfighting functions such as C2 or ISR. Due to the pressing demand on this activity, however, and the fact that the client's charter was to better integrate the Defence Capability Plan (DCP) projects to realise force level NCW capability, this team's focus was on developing a more *generic model* of NCW compliance suitable for use by the client over all projects. As NCW compliance is still a relatively new requirement in the Australian Defence Force it is anticipated that the focus will shift more towards a suite of methodologies and tool sets capable of meeting the many Capability Developments and Acquisition assessment needs.

Introduction

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). This document describes the theory and philosophy behind that framework. It is a companion paper to the NCW Risk Assessment Policy paper (Richer et al. 2006) that is also presented at this conference. The policy paper describes the motivation for this work and the NCW-RMR Stakeholder Framework, while this paper describes the NCW-RMR Assessment Framework. The Assessment Framework aims to mitigate against three key risks identified in the policy paper. These risks are:

NCW aspects of projects remain difficult to justify, despite the Department's focus on NCW.

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

NCW Issue 2. NCW aspects of projects often fail to combine to deliver an integrated NCW capability.

NCW Issue 3. NCW projects often fail to deliver a capability that can be used on delivery[1] due to the absence of:

[1] 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

NCW Sub Issue a.	major systems, which are delivered late, and
NCW Sub Issue b.	consideration of other Fundamental Inputs to Capability (FIC).

Compliance

Compliance in the context of capability *systems* and *systems of systems*, is defined essentially a process for managing and assessing a project, or collection of projects, against a framework of standards and regulations (e.g. systems *standards*[2], *protocols*, *architecture*[3] and *requirements*[4]). NCW compliance in the context of the ADF's *NCW integration plan* attempts to assess projects against a framework to ensure alignment with Defence Capability Strategy. Alignment with Defence Capability Strategy will allow achievement of the desired net-centric force-level capability across the whole of a *Capability Life Cycle (CLC)*.

The ADF is actively working towards establishing key enablers for a compliance assessment capability with the planned development of a *battlespace architecture, a mandated standards lists* and *a standards management framework* (ADF 2005 p. 17, 25). At the same time, across defence science and industry, initiatives for assessing the level of NCW compliance continue to move forward (Unewisse et al. 2005, 2006; Boyd et al. 2006). Meanwhile there remains the more immediate and pressing demand to support projects already transitioning through the Defence capability development process. Other compliance methods which are *not heavily reliant* on architectures and standards for assessing the NCW aspects of projects should therefore be considered.

Unewisse et al. (2006) propose a compliance model based on the design and analysis of systems and systems of systems. We extended this model based on a simple waterfall model of systems development covering three stages: *requirements*, *design* and *implementation*. Each of these steps occurs for both the system of system and the system. Ideally, the *design* of the system of system captures the *requirements* for the system. In practice, the process is a dynamic one, both iterative and evolving as the context, environment, standards, existing capability change the requirements and as the systems of systems strengths and limitations become understood.

We also distinguished two forms of assessment or, using Unewisse's terminology, forms of analysis. The first is the analysis of products against *production* standards

---

receive the capabilities it expects….examples include the Collins Class Submarine, Sea Sprite helicopters for the Anzac Class frigates and stand-off weapon systems for the F111 aircraft……,

[2] http://en.wikipedia.org/wiki/Standardization . In the context of business information exchange, 'standardisation' refers to the process of developing data exchange standards for specific business processes using specific syntaxes. Standards are characterised by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides benefit to the capability.

[3] http://en.wikipedia.org/wiki/Architecture, In modern usage…..explicitly *planned architectures* of human-made things such as *software*, *computer*, *enterprises*, *and databases*,….In every usage, an architecture may be seen as a *subjective mapping* from a human perspective (that of the *user* in the case of abstract or physical artifacts) to the elements or components of some kind of structure or system, which preserves the relationships among the elements or components.

[4] Definition: Compliance (regulation): In Management, the act of adhering to, and demonstrating adherence to, a standard or regulation. http://en.wikipedia.org/wiki/Compliance, accessed on 22 March 2006.

for that product. Within this model we term this *compliance analysis*. For example, the system of systems design might be captured in an architecture that has to meet architectural standards. The second form of assessment we refer to as *verification analysis;* that is, verification that the product meets the *requirements*. Figure 1 shows the relationship between these forms of compliance.

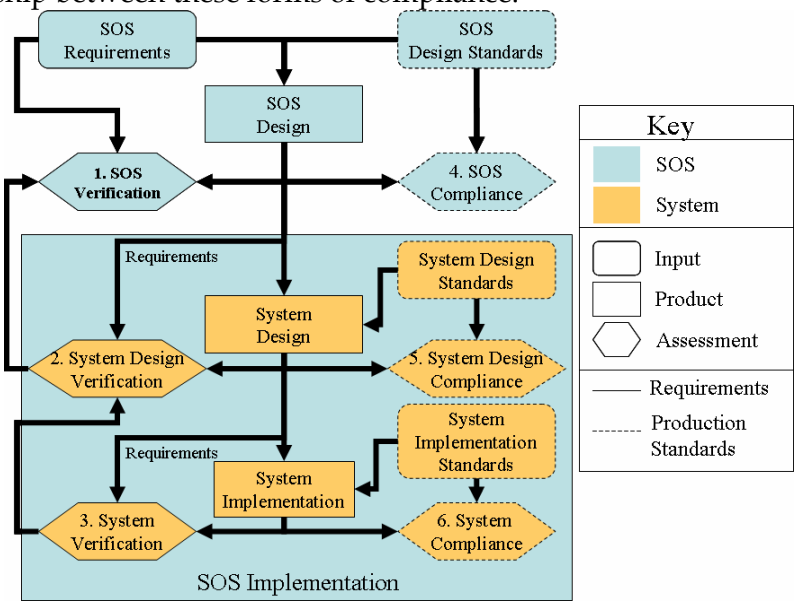

Figure 1: Forms of Compliance

We used this model to position those dominant international NCW compliance activities. Given the short time (six weeks) initially allocated by our client for the development of the compliance process, our own literature review was necessarily curtailed. Since then we have had the opportunity to review, draw upon and provide feedback into the literary work of Boyd et al. (2006).

In analysing these leading compliance models, we also considered the scope of each model. The authors are aware of some models—many developmental—that focus on specific warfighting functions such as C2 or ISR. However, due to the pressing demand on this activity, and the fact that the client's charter was to better integrate all the Defence Capability Plan (DCP) projects to realise force level NCW capability, this team's focus was on developing a more generic model of NCW compliance suitable for use by the client over all projects. Therefore, little time was available to fully review such specific models. Table 1 summarises our preliminary analysis of a suite of models national models as well as the emerging framework of the force-level NPI approach (Unewisse et al. 2006).

Australia has adopted a *learn-by-doing* approach (ADDP-D3.1, 2004) and, as discussed in Unewisse et al. (2006), this has led to the absence of clear system of systems requirements and difficulty in developing a system of systems design. This, in turn, leads to an absence of NCW requirements for the system (see Figure 1). Furthermore, as the science of NCW is still relatively adolescent, albeit complex, Australia is in the unfortunate position of being the recipient of competing approaches employed by other nations, some of which are prohibitively complex in terms of our needs, e.g. the US GIG. While other approaches are complementary, some involve slightly divergent views. This further complicates the Defence capability development compliance problem space in Australia where there is a lack

of endorsed NCW standards and design processes so that true compliance assessments (as in the RHS of Figure 1) are not currently possible. This means that none of the US approaches can be adopted. Furthermore, with regard to those models identified by Boyd et al. (2006) as our emphasis is on compliance and not on force-level design, we chose not to adopt the UK approach.

The closest analysis approach to our research objectives was that of the NPI suite of analysis approaches. Our team reviewed this collection to see how well it addressed the three NCW issues of interest. Issue 1 was only partially addressed. Issue 2, associated with delivering an integrated capability, was well addressed. Issue 3a, associated with the coordination of the delivery, was not addressed. The NPI suite provided a mechanism for identifying the top priority systems based on the implied system of systems design (Capability Cross Impact Analysis) as well as a mechanism for determining system of systems designs to meet a variety of force-level operational requirements for future capabilities (Organisational Analysis). However, Organisational Analysis requires a significant analysis effort and expertise in capability development not yet resourced or routinely practised at a sufficient level in capability development. While we recognise the benefits of this approach, we also wanted to be able to provide a simple mechanism for checking the justification of a project that could be determined from the evolving capability development documentation package of a project (as-far-as-possible).

As illustrated in Table 1, elements of the NPI methodology appeared to map to our requirements, but did not completely fill some of these. Therefore, we decided to develop an overarching framework that addressed our issues and to concentrate our efforts on those areas that were outside the scope of, but which could be used to complement NPI research at a later stage.

However, there were also some differences in the assumptions of the NPI and the approach we developed. The *first* is that the NCW-RMR process is focused on the *analysis of the system* within a system of systems context while the NPI is predominately focused on *analysis of the system of systems* building on an understanding of the system. These differences do, however, have a common element—an understanding of the way the system is linked into the system of systems. Because of this we have developed some areas in common with the NPI.

The *second* difference lies in the fact that we wanted to develop a method that could be applied to documents by systems engineers who lack specific NCW expertise following a limited amount of training based primarily on documentation. This development was necessitated by staffing constraints within the NCWPO and has led to the creation of a different assessment philosophy.

The *third* difference lies in the fact that we wanted to create a methodology that did not require the specification of standards for interfaces. Our philosophy is based on the assumption that standards will change during the acquisition of a system and that alternative means of assuring compatibility of the interfaces is required. In contrast, the NPI builds on the approved Defence Standards List (DIE ATSL 2005).

Methodology	Form of Compliance Assessment (Figure 1)	RMR NCW Issues Addressed	Methodology Focus Area	Comments
NPI Methodology (Unewisse et al, 2006)	Aligns with compliance forms 1 and 2 as shown.		Suite of analysis approaches covering the following:	
• Capability Cross Impact Analysis	1.SOS Validation[1]	1. (high dependency systems only)	Prioritisation of analytical effort.	Used to identify systems of interest for detailed analysis through a series of CI workshops of stakholders and IPTs to collaborate and prioritise in tiers the deficencies of projects considered essential to future SOS design e.g. T1-critical and T2- major systems, T3, etc.
• Capability Qualification Analysis	2.System Design Validation	3. (needed vs planned)	Project level design analysis to assess NCW fitness of capabilities in isolation.	Uses detailed question lists. Generic issues cover Information Management and Systems Integration.
• Capability in Context Analysis	1.SOS Validation	2. (requirements)	Focuses on interface quality and usage requirements of a system within the SoS context.	Support for project-level capability missions and tasks.
• Organisational Analysis	1.SOS Validation	1. 2.	Focuses on the ability groups of selected projects to achieve specific objectives.	Support for organisational missions and tasks. This methodology used as part of the NPI apparoach highlights the importance of force level design aand the need for force-level capability defintion documentation as opposed to the current practice of project level design and definition.
• Holistic Risk and Vulnerability Analysis	1.SOS Validation	Summary of all Issues	Risk at the whole-of-capability and force-levels.	Holistic systemic risk and vulnerability analysis capture those NCW-capability "failure modes" and IDs those underlying causes. This process summarises the risks identified using the above methods.
US DoD Net-Ready (NR)-KPP[2] Methodology	Aligns with compliance forms 1, 4, & 6 as shown. [2]		Suite of performance based methods to assess compliance with US DAF architecture and standards.	Ref: US DoD Instruction 5000 Defence Acquisition Guidebook 2004. http://akss.dau.mil/DAG/Guidebook /IG_c7.3.4.asp
• NCOW Reference Model (RM)	4.System Design Compliance[3]	-	A means to describe a projects degrees of net-centricity and abiliy to comply with GIG architecture and standrards.	This identifies terminology, architectural products etc that are to be used. http://akss.dau.mil/DAG/Guidebook/IG_c7.3.4.1.asp
• Net-centric Checklist / Net-Centric Enterprise Solutions (NESI)	6. System Compliance	-	Provides a net-centric compliance checklists for technical guidance and enterprise design to build NC capabilities.	This identifies coding and other standards to which the system must comply.
• GIG Key Performance Indicators (KPI)	1. SOS Validation 4. SOS Compliance	-	Configuration control audit approach to interoperability compliance of capability development documentation e.g OCD, FPS and TCD.	This is an interesting blend of 1 and 4 where the assessment is based on consistency with key elements in the SOS Design. Focus areas are Communications, Computing and Services.
• DoD Information Assurance (IA)	5. Systems Design Compliance [4]	-	Focus is Information Assurance.	Series of IA baseline and supporting audits to ensure a compliance to statutory requirements. http://akss.dau.mil/dag/DoD5000.asp?view=document http://akss.dau.mil/dag/Guidebook/IG_c7.5.9.1.asp
UK NEC Benefit Analysis (Boyd et al, 2006)	1. SOS Validation*	1, 2.	*This method appears to be focused more on analysis to support the development of the design, rather than to analyse an existing design.	Capability requirements vs effectiveness vs investment options approach incorporating tailored assessments developed through workshops and benfits mapping.

Table 1 Analysis of Compliance Models

Notes:

[1] Although Australia does not have an NCW model to drive requirements or an endorsed systems of systems design as noted by Unewisse et al. (2006), this analysis methodology still fits at this level because it looks at the importance of systems in the implied systems of systems design.

[2] Compliance of net-ready attributes of capability at systems and SoS level using reference models, net-centric checklists, KPIs and IA measures below.

[3] This applies to the information publicly available. They could also be used for system of system design compliance. From the publicly available information it appears that sections 1 and 4 might be covered to some degree.

[4] This method comprises a series of IA audits against Baseline IA requirements models and compliance to the Clinger-Cohen Act 1999

Assessment Philosophy

There are several approaches that could have been adopted in the assessment of NCW compliance. These include differences in the way the assessment could have been undertaken (questions, expert opinion, analysis, interviews, modelling and simulation) and the results aggregated (weighted sum, maximum value, etc). The approach chosen reflects a balance between the pragmatic constraints (the NCWPO plans to use contractors to perform assessments), the desire to enable simple expansion of the framework, and the approach that would theoretically deliver the best result.

In order to enable contractors to perform assessments in a relatively short time-frame, the approach used in the new components of the framework is based on a series of questions, the answers to which can be found in the available documentation. This approach is consistent with those used for most of the components of the NPI methodology and is also with that used in the US NESI approach.

In the NCW-RMR, in addition to providing a simple Yes/No response to questions, default remedial actions are provided to rectify any problems identified. To support more complex situations while still using simple Yes/No responses, four standard mechanisms for moving between the questions are used:

- Go to the Next Question;
- Skip the Next Question;
- Go to the Next Category of Questions; and
- Go to Category X, where X is one of the following categories.

These responses can be understood by a tool such as the concept demonstrator developed by Benjamin Cobb (2006) which can automatically navigate through the questions.

The approach used to aggregate the results is based on the maximum (or worst case) value. This approach was used because it is simple for decision-makers to understand and also allows the results from other analysis to be incorporated with ease. This approach is also suitable for use in the absence of a theory of the relative worth of various elements of the analysis approach. A simple summation of results could have been used, but where there are many criteria this does not give sufficient weight to single 'show stoppers'. Thus the approach taken is to categorise the results as 'No Action Required', 'Action Required' and 'Priority Action Required' depending on the relative importance of the required action. If there are any priority actions required, the project is deemed to be 'High Risk'; if actions (with no priority attached) are required then it is deemed to be 'Medium Risk' and if no action is required it is deemed to be 'Low Risk'.

In order to facilitate the aggregation and make it easy for committees to understand the results, the questions are grouped at three levels or areas which consist of multiple question criteria—which themselves consist of multiple categories. The categories are mainly used to simplify navigation through the questions, as users

found it difficult to apply early versions of the question list. The theory behind the areas and criteria is described in this document.

Assessment Scope

The objective of the approach being developed was to provide an NCW assessment of all projects going before committee. In order to simplify the scope of the initial framework, a decision was made to focus, as far as possible, on the common NCW elements of projects. This meant that infrastructure and applications projects would be treated more or less in the same manner. It also meant that conditions specific to particular domains—such as ISR or C2—were not included, because other researchers in Australia are taking up the high-level framework and are starting to develop subordinate frameworks for specific domains.

Assessment Areas

The proposed analysis framework comprises four assessments areas, three of which are based on the idea of encapsulation, as illustrated in Figure 3 Diagram *One*. As this diagram indicates, the project is examined as a single entity or a black box, which requires interfaces with other capabilities. This model is designed to address NCW Issue 1. Diagram *Two*: the box is opened up sufficiently to show the detail of the interfaces addressing NCW Issue 2. Diagram *Three*: the box is opened up completely so that the major systems and other Fundamental Inputs to Capability can be examined thereby addressing Issue 3. To date, questions have only been developed for the first of these models, and some questions for the second model.

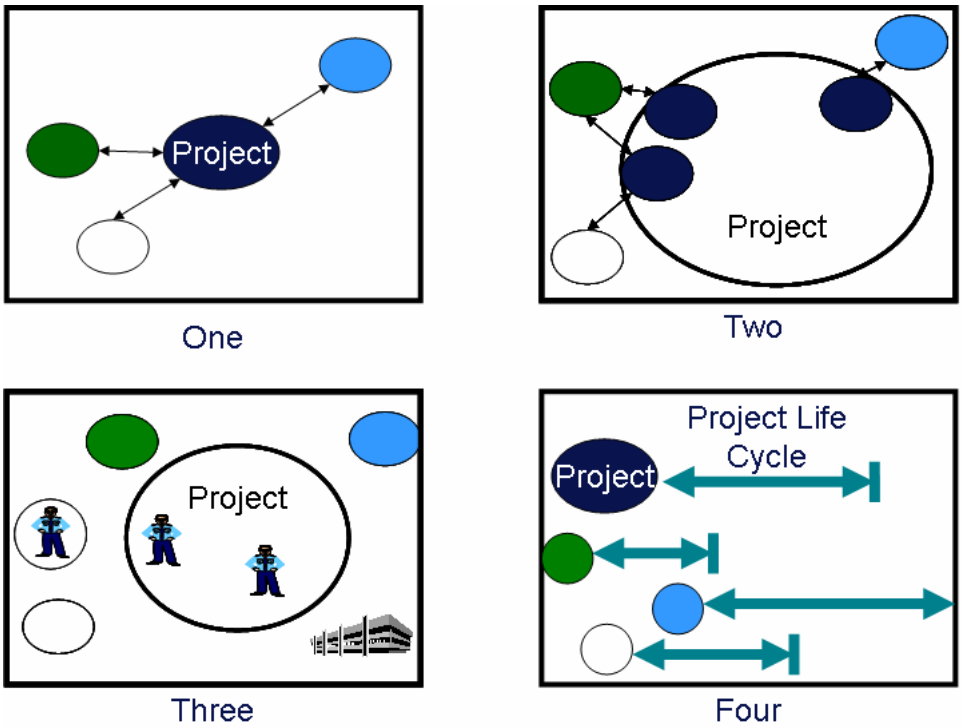

Figure 2 Analysis Areas

Diagram *Four,* adds a *temporal dimension*. The project in this area is examined as part of the whole Defence acquisition strategy. This should include, among other aspects, the cost of acquiring systems-level DCP capabilities for systems of systems force-

level effect and the impact of such a program on the acquisition investment strategy. Availability of resources (including finance) and the appropriateness of the delivery time-frames should also be examined. In practice, the information required to perform some of these assessment areas is available at a similar time to the black box assessment, so it will be the second area analysed.

If the first two areas are grouped together, these four areas align with the areas of the System of Systems Interoperability Model (SOSI) (Levine et al 2003)—Programmatic (cf Four), Construction (cf One and Two), and System (cf Three) interoperability.

These areas also map well to the problems that had been encountered in the acquisition of NCW capabilities. These included: problems with defence committees understanding the capability to be delivered by NCW projects; capabilities being delivered that could not be integrated into the defence system; problems with FIC as raised in the first paper; and projects being delivered before the supporting infrastructure was available.

From this we derive the four major areas of assessment described below:

1. **NCW Requirements Analysis –** This analysis 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. It is intended to ensure both that projects are ready to go before the relevant committees and that the scope of the project has been justified. (In order to enable other projects to correctly identify interfaces to this project, it also identifies those major NCW elements being delivered by the project.)

2. **NCW Force Analysis –** This analysis area is focused on assessment of the project in the context of the Capability Life Cycle (CLC) and the DCP, and covers issues such as how the capability option fits with other capability options. This area aims to provide information on the dependencies between projects in the DCP so as to facilitate decisions on scheduling, resources, and revising the DCP. Minor Capital Projects, Rapid Acquisition, and Rapid Prototype Development and Experimentation (RPD&E) tasks are assessed against the DCP projects and not against all other Minors, Rapid Acquisition and RPD&E projects.

3. **NCW Systems Analysis –** This analysis area explores in more detail the requirements placed on the capability by outside capabilities that are in service, under development, or planned—and vice versa. This dimension corresponds roughly to the *Network* dimension of the *NCW Roadmap*.[5]

4. **NCW FIC Analysis –** This analysis area explores whether there are any *Fundamental Inputs to Capability* issues with the introduction of the capability and its NCW elements. This area could include training to exploit new NCW elements and the processes, doctrine, etc. that result. This dimension corresponds roughly to the *Human* and *Networking* dimensions of the *NCW Roadmap.* These areas are grouped for two reasons: first, because they are difficult to separate; and second, because additional activities have been

[5]*ADF NCW Roadmap* endorsed for release by the Defence Minister, Senator Hill, in November 2004.

identified by the NCW Implementation Team (NCW IT) and in the *NCW Roadmap* to address these areas.

NCW Requirements Analysis (NRA)

The rationale for NCW Requirements Analysis is based on the need to ensure that, prior to approval for expenditure of significant funds, all proposed options with NCW capabilities have been checked for consistency, completeness, alignment, and justification with the existing ADF NCW implementation strategy including addressing such areas as known NCW capability gaps, aspirational NCW Architectures and Interface requirements. Identification of inconsistencies at this level will reduce the number of revisits currently being experienced by projects within the DCP and decrease the backlog of projects still in the early part of the requirements phase.
NCW Requirements Analysis consists of two criteria, namely *Background* and *Justification*, which are divided into a number of categories of questions.

The first—*Background*—is designed to determine whether 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.

The second—*Justification*—is designed to examine the justification for the NCW components of the project and its interfaces as well as the consistency and completeness of these interfaces. Assessing this criterion involves consideration of the justification for the project and the interfaces, and the completeness and consistency of the interfaces. The objective is to ensure:

a) that the project will deliver the required NCW capability,
b) that the project will deliver the interfaces required by other capabilities, and
c) that other projects will deliver the capability required by the project being assessed.

Potentially, there are several sources of information on a project, although the different sources may contain inconsistencies. These include the project of interest (let's call it project A) and, in particular, its official or draft documentation; other projects and capabilities, particularly those that intend to make use of the project, whose expectations may not be realistic (let's generically call this project B); and the proposed NCW Architecture. Inconsistencies in the information and expectations between these information sources constitute a risk that the project will not integrate as expected into the future NCW force.

Figure 4 shows a potential initial state. The documentation for project A (shown as a yellow document labelled 'A' in Figure 4) contains most of the information about project A (shown in black) and an interface with two other projects. The NCW Architecture recognises the need for the projects, but only contains one of the interfaces from project A's documentation. It also includes an interface with another project. That is, it contains a requirement not identified by project A. Finally, project B's documentation (shown as a yellow document labelled 'B' in Figure 4) lists an interface requirement with project A which has not been recognised by project A or in the NCW Architecture.

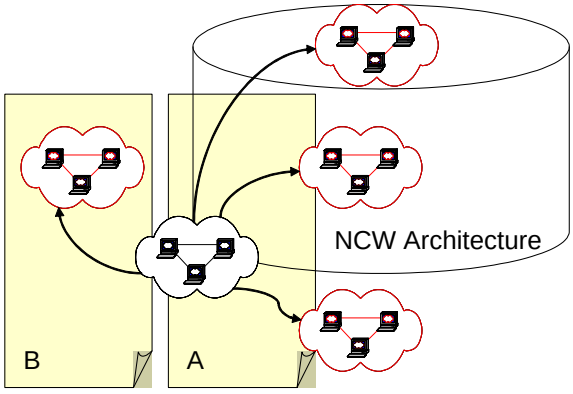

Figure 3 Initial State of Interface Capture

These differences indicate a substantial risk that the project will not be able to deliver to its full potential in an NCW environment and that other capabilities will also suffer as a consequence. When an NCW Architecture exists, it is project B's responsibility to ensure that the project's requirements are reflected in the NCW architecture. However, when there is no endorsed NCW architecture it is the responsibility of both projects to develop complete and consistent requirements. The questions in this criterion try to identify such problems and propose appropriate actions. More generally, they also try to ensure that the project's NCW characteristics are appropriate.

The process used is summarised in Figure 4. If there is an NCW Architecture (NCW Arch), the process on the left is used. If there is no NCW Architecture, the process on the right is used. If there are discrepancies between the project's documentation and the NCW Architecture, then elements of both may be used.

Initially the team proposed to separate the assessment of the project justification and interfaces. However, during an evaluation (discussed below) it was found that this caused confusion and revisiting areas of the documentation. Closer analysis of the problem identified the interactions shown in Figure 4 and they were combined to enable the flow of the questions to be simplified.

While the project and interfaces, or the interfaces' completeness and justification, could be assessed separately, they have been combined into one category because of the interactions between them as shown in Figure 4.

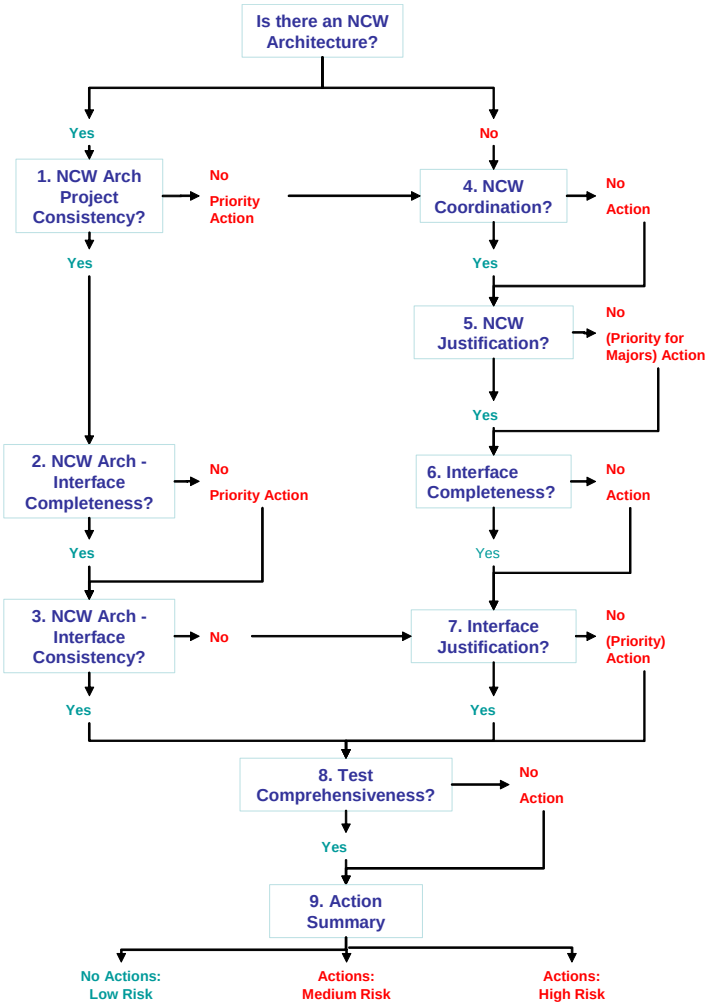

Figure 4 NCW Justification Process

NCW Force Analysis (NFA)

The rationale for NCW Force Analysis is based on the need to ensure that, at the early stages of entry into the DCP, projects are scrutinised for consistency and alignment with the aspirational network-centric needs of the future force in areas of levels of interoperability; resources issues to achieve such a level of connectivity; cross-project dependencies and prioritisation needs; and the levels or degree of adaptability each capability planned for introduction will have to support an operational force.

The NCW Force Analysis area criteria currently consist of: *Interface Responsibilities*, which assesses how responsibilities for providing the interface have been divided; *Timeliness*, which assesses whether infrastructure projects will be delivered before those that will rely on them; and *Resources*, which assesses the suitability of available personnel and financial resources to deliver the required NCW capability. However, given the small number of questions in each area, this breakdown has come under review. In addition, further investigation of the SOSI model may reveal additional categories of questions that could be incorporated.

NCW Systems Analysis (NSA)

The NCW Systems Analysis area is concerned with systems interoperability and several models were reviewed in order to determine an appropriate set of criteria. As shown in Table 1 below, the models considered were the ISO 7-layers of Information Systems model (ISO/IEC, 1994), the Levels of Information Systems Interoperability (LISI) model[6] (C4ISRAFWG, 1998), Tolk's (2003) model of coalition interoperability, and a miscellaneous collection of models that had been proposed by various other researchers interested in our approach. These included: the NCW Grids; Standards for Open Architectures, Imaging, Information Communications Technologies, Encryption; the Technical Risk Assessment approach used by the ADF and the endorsed Defence Architecture Framework.

Because of a desire not to focus on specific standards that could be out of date by the time a system was delivered we did not consider the standards other than to ensure that there were points at which the various standards could and should be applied.

Tolk's Political and Operations level were thought to be at too high a level for consideration in the design of systems, while Doctrine is covered by the NCW FIC analysis. Tolk's Procedures and Knowledge have been combined into what we term *Operator Connectivit*y which is concerned with ensuring that the human elements in the system are able to perform their required roles. Applications and Presentation from the ISO model are combined into *Applications,* as in the LISI model, as sufficient detail to separate the two will not always be available in capability development documentation. *Information Management* is an important area that goes beyond consideration of what information is exchanged to also include the means of exchange. It is combined with Tolk's Data because the information management policy may affect the format in which data is exchanged. Session, Transport and Network from the ISO model were believed to be important, but potentially at too low a level for the capability process, so these were roughly mapped into a new Category called *Network Management*. Finally, the ISO physical and data link categories are combined into a single category, *Physical and Communications Connectivity,* again because of the level of resolution available in many capability documents.

[6] The LISI model was independently recognised as one of the best models of systems interoperability by Kasunic (2001).

Adopted	ISO	LISI	Tolk
			Political
			Doctrinal
			Operations
Operator Connectivity		Procedures	Procedures
			Knowledge
Applications	Applications	Applications	
	Presentation		
Information Management		Information	Information
		Data	Data
Network Management	Session		
	Transport		
	Network		
Physical and Communications Connectivity	Data Link		
	Physical		

Table 2 NCW Systems Analysis criteria -comparison to existing methods.

NCW FIC Analysis (NFICA)

The DCM 2005 provides guidance on the requirement for projects to determine at the early stages of development the impact of introducing a new capability into Defence through the lens of the eight Fundamental Inputs to Capability (FIC). Failure to address FIC elements has resulted in new capabilities stalling at the in-service testing and acceptance stage of the acquisition phase.

It is proposed that the current Australian FIC categories be used. To date, no work has been undertaken to date by the authors on identifying questions for this area.

Evaluating NCW RMR Framework

The purpose of this activity was to evaluate selected NCW-RMR criteria and question lists designed to be employed by the NCWPO against DCP projects entering the capability proposal first pass (CPFP) stage.[7]

The methodology chosen to support the evaluation of the RMR had to be able to:

- result in more refined and tighter criteria, categories and questions;
- be useful across all analysis areas of the NCW risk analysis framework; and
- have the ability to be easily employed by NCWPO assessment desk officers.

The outcomes of the evaluation were a combination of the following:

- acceptance of the analysis area with changes to the criteria,
- acceptance of the criteria with changes to the question structure, and
- acceptance of the questions structure with changes to the questions.

The method used to evaluate the RMR model shown at Figure 6 employed two approaches, namely:

[7] A direct comparison with the NPI was not possible because it was being upgraded to support joint analysis at the time.

- *structured based approach* which stepped logically through the analysis questions—the approach intended for use by the NCW PO compliance team; and
- *broad (criteria) based approach*, a less structured approach focused on the high-level analysis areas to capture any information contained within the project documentation relevant to NCW but not captured by the analysis questions.

Both approaches also identified relevant sections of project documentation that cover compliance and integration issues. The overall aim of the evaluation was to achieve a more comprehensive set of NCW compliance questions for the areas reviewed.

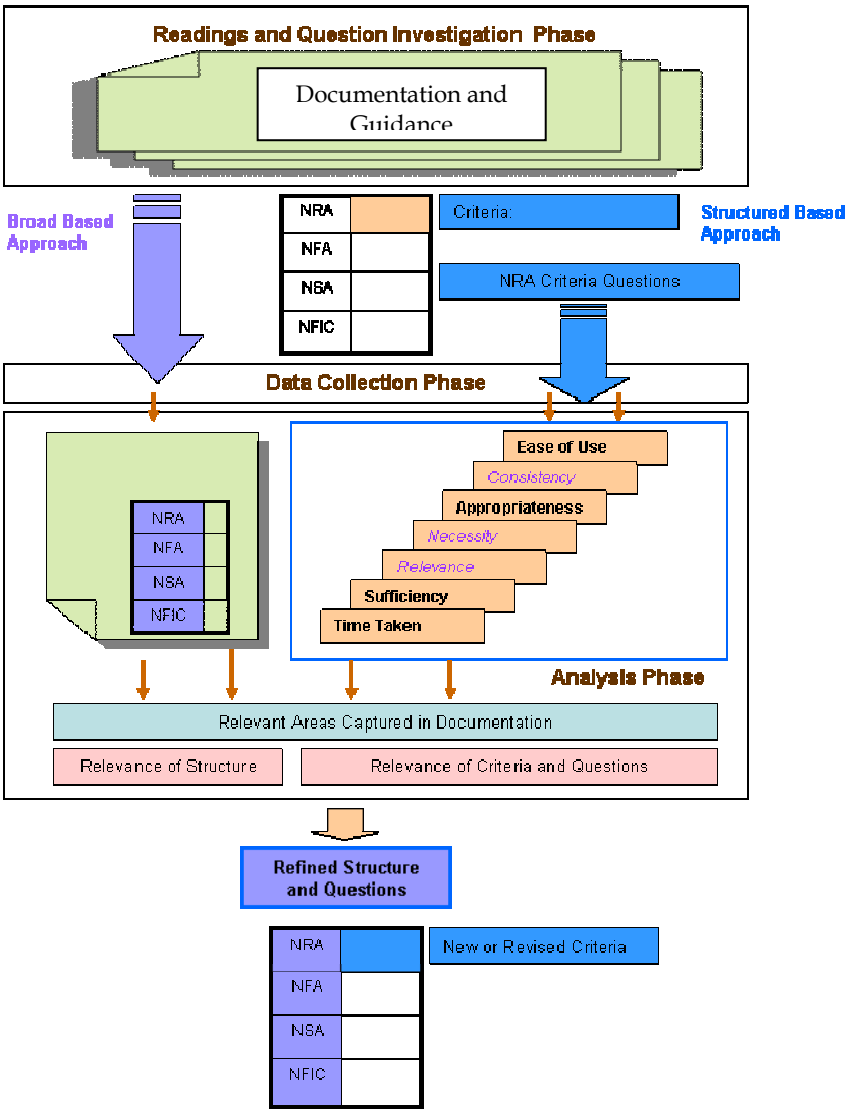

Figure 5 Complementary evaluation methods employed

The Evaluation Criteria

The trial was designed to examine the suitability of the proposed compliance process from the following analysis perspectives:

- the suitability to employ the two separate evaluation approaches against the selected analysis area to identify improvements and additions to the criteria and questions. This parallel approach enabled a relative assessment of the proposed approach using the criteria.
- the ability to compare the two approaches to identify further improvements and additions to the criteria and questions used.
- the ability to assess the suitability of the questions according to the trial criteria in Table 2. Here metrics 1-3 were assessed on a 5 point scale, 1 being the best possible rating and 5 the worst.

These metrics were employed for this first trial and are proposed for subsequent trials to be conducted as the other three NCW Framework Analysis Areas evolve. All of these metrics were employed in the structured based approach with only some of these metrics during the comparative analysis. An additional measure, inter-rater reliability, should also be incorporated as the NCW-RMR process matures.

Metrics	Scale	Description
1. Ease of Use	1 to 5	The degree of difficulty and time taken to fully understand and find an answer to the question.
1a. Consistency	1 to 5	Extent to which the questions are in line with and complementary to prior and preceding questions.
2. Appropriateness	1 to 5	Whether questions are apposite for gaining useful and usable information at this DCP stage.
2a. Necessity	1 to 5	The extent to which the question is essential yet discrete enough for investigating the Capability Development Documentation (CDD) while supporting the required NCW compliance criteria.
2b. Relevance	1 to 5	Whether questions and context are consistent with what is expected of projects at this DCP stage.
3. Sufficiency	1 to 5	Extent to which the questions investigate the NCW compliance issues in the CDD package and support the NCW Integration Plan.
Time Taken (Overall)	min/hrs	The time taken by user to read into and develop sufficient knowledge from the CDD packages to apply the analysis model.

Table 3 Trial Metrics

The evaluation approach essentially tested the ability of the chosen criteria, categories and question sets to support NCW integration assessment at the proposed stages of NCW review in the CLC process covered in Richer et al (2006). The view is that the structured approach does provide feedback on the suitability of the analysis area under review and, as will be shown in the findings, the ability to revisit and refine the structure and composition through the lens of the methodology employed is appropriate for use by NCWPO staff officers during the development approach and provides instant feedback on whether the team is heading in the right direction (i.e. the development of a suitable NCW assessment framework and process for the client.).

Results

The results of the assessment are summarised in Table 4 below. For the question-based approach, these were determined for each question and then averaged for the

summary table. For the criteria-based approach, this was done for the criteria as a whole and averaged over the two criteria. Where the assessment areas were difficult to apply or were not relevant for the criteria-based approach, the corresponding field in the table is shaded in grey.

Issues identified are viewed through two lenses: the total, and those that were only identified by one of the methods (unique issues). Unique issues identified in the criteria-based approach signal the need for additional questions in the question-based approach, while unique issues in the question-based approach indicate the value of a more structured approach.

Assessment Area	Question-Based Approach		Criteria-Based Approach
	Legitimacy	Interface Requirements	
Ease of Use	4.4	3	3 (Given sufficient expertise)
Consistency	1.7	1.2	
Appropriateness	1.5	1.2	
Necessity	1.4	1.2	
Relevance	1.5	1.2	
Sufficiency Issues Identified – Total (Unique)	1 (0)	2 (0)	4 (0 – variations on a theme)
Time Taken	See below.		
Questions With Recommended Changes (Based on initial analysis)	Change: 5 Drop: 2 Add: 3 Total (Original): 13	Change: 5 Drop: 0 Total: 11	

Table 4 Results from the Evaluation

As the results indicate, both approaches were quite difficult to use. The analysts suggested that this was due to their lack of familiarity with the style of the documents under review. This led to difficulty in determining where to search for the answers to the questions. This problem is also reflected in the consistency scores, as the same section of the document was often referred to at different times during the review. The problem was addressed by restructuring the questionnaire. The next activity involved identifying the major sources of information in these documents. This was undertaken with two objectives in mind. The first objective involved the realisation that the data collection activity assists the analyst to develop an understanding of the document. The second objective was to demonstrate that the information collected forms a resource that can be used not only during the analysis of the project, but also in terms of a data repository that can be referenced when analysing the system of systems aspects of other projects. Anecdotal feedback from the lead in the group responsible for applying the methodology indicates that it has achieved the first objective, although the second is still to be tested.

The second problem involved the difficult task of trying to separate the conduct of the NCW-RMR and the conduct of the assessment activities. In addition to its impact on the questionnaire's ease of use, this also led to problems in determining the time taken to complete the activities. In future analyses, we recommended that one person performs the NCW-RMR assessment and another observes or records the

activities. The NCW-RMR analyst could also be interviewed once he/she has completed the assessment. This would free the analyst from the experimental objectives and add to the independence of the evaluation.

Resulting Assessment Areas

Based on the findings in both the structured and criteria based evaluation of the NRA analysis area, the team members developed a refined NRA as detailed in Table 4. These are considered more appropriate for the breadth of capability development projects[8] the client's assessment team will be required to review, monitor and assess as part of the Capability Development Group's NCW integration requirements. This revised NRA now consists of three criteria with supporting categories and question lists. This NRA area is being used to a limited extent by the client as well as forming part of a NCW compliance training package for the assessment team.

NCW Requirements Analysis Area	NRA Criteria	No of Categories	No of Questions
NCW Requirements Analysis	Background	2	8
	Justification	8	24
	Options Implications	4	33

Table 5 Resulting NCW Requirements Analysis Area

Conclusions

The NCW-RMR model described in this paper has been used in the analysis of two projects. While successful in identifying a number of issues in both projects, a number of limitations were also identified and addressed. Staff at the NCWPO have been successfully trained in the revised methodology and are currently adapting it to suit their evolving requirements.

One area being investigated is the relationship between the NCW-RMR and the NPI. As previously discussed, the NPI is focused on the system of systems analysis and the NCW-RMR on the project. Despite this there is some overlap. The following table 6 provides the authors' view on the relationship between these two processes. The term 'NCW-RMR' is used to refer to the appropriate section of the NCW-RMR. In addition, other methodologies are drawn from the NPI.

[8] The revised NRA analysis area can now be used by capability majors, minors, rapid prototype and development as well as rapid development projects considered having an NCW capability .

Major Activity	Minor Activity	Methodology
Project Selection		Capability Cross Impact Analysis
NRA	Background	NCW-RMR
	Justification	NCW-RMR
	Options Implications	NCW-RMR
NFA		
NSA	Physical and Communications Connectivity	Capability in Context *and* NCW-RMR *or* Capability Qualification Analysis – Technical
	Information Management	NCW-RMR *and* Capability Qualification Analysis – Information Management
	Network Management	Capability Qualification Analysis – Information Management
	Applications	C2: Capability Qualification Analysis – C2 Other: Under development by other researchers at DSTO.
	Operator Connectivity	Organisational Analysis
Project Summary		NCW-RMR
Systems of System Summary		Holistic Risk and Vulnerability Analysis

Table 6 A Comprehensive Compliance Approach

Acknowledgements

Many thanks to Mark Unewisse, Ant Perry and Shaun Wilson for their discussion on compliance and the NPI, and for their willingness to share draft versions of their documents. Thanks to Abdel El-Sakka for his contribution to the FIC area development. Thanks to Terry Moon and Jason Scholz for sharing their ideas on compliance and a special thanks to Les Vencel and Paul Pappas for reviewing an earlier version of the NCW-RMR. Some of their ideas have found their way into this version of the NCW-RMR, others remain possibilities for future incorporation, particularly as variants for different warfighting functions are developed.

References

Department of Defence (2004), *Enabling Future Warfighting: Network Centric Warfare Concept (ADDP-D.3.1)*, Defence Publishing Service, Canberra, Australia.

Department of Defence (2004), *The ADF Network Centric Warfare Roadmap,* Defence Publishing Service, Canberra, Australia.

Department of Defence (2003), *Defence Procurement Review*, 2003, Defence Publishing Service, Canberra, Australia.

Department of Defence (2005), *NCW Roadmap 2005*, Defence Publishing Service, Canberra, Australia.

Boyd, C. S., Wilson, S. A., Williams, W. R., & Skinner, D. J. (2006), *Network-Centric Warfare Prioritisation & Integration – Review of Assessment Approaches*, ACPL-REPORT-20-2005-J53, Aerospace Concepts Pty Ltd, Canberra, Australia.

C4ISR Architecture Working Group, (1998) *Levels of Information Systems Interoperability (LISI)*.US DoD, March 1998

Cobb 2006, *NCW Capability Assessment Process Tool (A Prototype Demonstrator), User Support Manual,* Version 1.0, Draft, a DSTO work in progress March 2006.

Australian Defence Force 2005, *Defence Capability Manual*, Defence Publishing Service, Canberra, Australia.

Information technology – Open Systems Interconnection – Basic Reference Model: The Basis Model. ISO/IEC 7498-1:1994 www.iso.org accessed 28 March 2006.

Kasunic 2001, *Measuring Systems Interoperability: Challenges and Opportunities*, Software Engineering Institute, Carnegie Mellon University, USA.

Levine, L., Meyers, B. C., Morris, E., Place, P. R. H., & Plakosh, D., 2003, *Proceedings of the Systems of Systems Interoperability Workshop (February 2003),* CMU/SEI-2003-TN-016, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA.

Richer, W., Kohn, E., and Kingston , G., *NCW Risk Management Policy and Process,* 2006 ICCRTS, March 2006.

Shekmar and Kreger 2004, *Net-Centric Checklist*, Version 2.1.2 2004, Office of Force Transformation, US DoD, 31 March.

Tolk, A., *2003 Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability*, 8th International Command and Control Research and Technology Symposium, Washington DC, www.dodccrp.org

Unewisse, M., Wilson, S., Perry, A., and Boyd, C. 2006, *An Australian Approach to Assessing Force-Level Network-Centric Warfare (NCW) Readiness*, CCRTS.

Unewisse, M. 2004, *JP 5000: A Review of the Progress Towards an NCW-Capable Land Force*, in Proceeding of the Land Warfare Conference 2004, Department of Defence, Adelaide, Australia.

Defence Acquisition University, *Defence Acquisition Guidebook Version 1.0*. 17 October 2004, http://akss.dau.mil/DAG/Guidebook/IG_c7.3.4.1.asp US DoD, accessed 28 March 2006,