Australian Government
Department of Defence
Defence Science and
Technology Organisation

TECHNICAL RISK ASSESSMENT HANDBOOK

DSTO Science and Technology for a Secure World

Projects and Requirements Division
Defence Science and Technology Organisation
Fairbairn Business Park Department of Defence
Canberra ACT 2600 Australia
Ph: 02 61286307

Approved for Public Release

Preface

Overview

The *Technical Risk Assessment Handbook* (TRAH) provides Defence personnel and relevant stakeholders with a process and best practice guide to the assessment of technical risks for major capital acquisition programs.

The *Defence Procurement Review 2003* (known as the Kinnaird Review) recommended that Defence consideration of new acquisitions include *'comprehensive analysis of technology, cost and schedule risks'*. The Review also recommended that *'Government needs to be assured that adequate scrutiny is undertaken ….by DSTO on technology feasibility, maturity and overall technical risk'.* As a result, the Chief Defence Scientist (CDS) became responsible for providing independent advice to Government on technical risk for all acquisition decisions.

In 2005 the Defence Science and Technology Organisation (DSTO) developed an approach to Technical Risk Assessment (TRA) and certification. Since then, Capability Development Group (CDG) and DSTO have worked together to develop improved procedures for managing technical risks for acquisition projects which are described in the *Defence Capability Development Handbook (DCDH)*. This TRAH describes improvements to the TRA process which capture the lessons learned from conducting TRAs since 2005.

Scope

The TRAH describes the framework in which DSTO Project Science and Technology Advisers report the technical risks identified and assessed in major capital acquisitions. It also explains the processes for developing the supporting documentation needed to inform the project and the Government. The Handbook does not discuss other programs (such as the Minor Capital Acquisition Programs or the Major Capital Facilities Program) for which CDS is not required to certify the technical risk.

This Handbook should be read in conjunction with the *Defence Capability Development Handbook (DCDH),* which describes the capability needs and requirements development process and the role of technical risk assessment in that process.

Tailoring the handbook

Defence has a wide range of complex projects, and risk assessment is not a 'one size fits all' approach. In developing technical risk assessments, the risk assessor should apply appropriate context and understanding to individual projects. While the approach outlined in this Handbook is sufficiently general to be applicable to the majority of projects, it may need to be tailored for specific projects. This should be done in consultation with the Studies Guidance Group (SGG) of DSTO Projects and Requirements Division, who are responsible for technical risk policy and process in DSTO.

It is my intent to regularly review and update the TRAH to ensure it remains aligned with the broader capability development processes as set out in the DCDH, and to ensure the TRAH remains best practice.

Jim Smith
Chief Projects and Requirements Division

Contents

Chapter 1
Introduction

1.1 Technical risk is a major factor to be considered in the acquisition of new defence capabilities. While the application of developmental technology offers potentially significantly enhanced capability over existing systems, it can also lead to excessive delays and cost blow-outs. Following problems with the development of the Collins submarine in particular, Defence commissioned a review with the objective of recommending improved acquisition processes and better managing the acquisition of developmental systems, including their inherent technical risks. The *Defence Procurement Review 2003* (known as the Kinnaird Review) recommended that Defence strengthen the two-pass system for new acquisitions to include *'comprehensive analysis of technology, cost and schedule risks'*. The Review also recommended that *'Government needs to be assured that adequate scrutiny is undertaken ….by DSTO on technology feasibility, maturity and overall technical risk'.* As a result, the Chief Defence Scientist (CDS) became responsible for providing independent advice to Government on all acquisition decisions.

1.2 The *2008 Audit of the Defence Budget* (known as the Pappas Review) identified technical risk as the major cause of post-approval slippage and a significant cause of cost escalation, and proposed that Defence should accept technical risks only where there is significant capability benefit to do so, and further improving technical risk management practices would help reduce schedule and cost escalation.

1.3 In 2009, *The Response to the Report of the Defence Procurement and Sustainment Review* confirmed that *'the Chief Defence Scientist's responsibility for providing independent advice on technical risk remains unchanged'*.

1.4 Accordingly, Capability Development Group (CDG) and the Defence Science and Technology Organisation (DSTO) have developed appropriate policy and processes for assessing the technology maturity, feasibility, and technical risk of projects at appropriate points in the Capability Systems Life Cycle (CSLC), as described in the *Defence Capability Development Handbook (DCDH)*. Based on experience to date, CDG and DSTO have implemented an improved procedure for managing technical risks in projects which has been incorporated into the DCDH.

1.5 The purpose of conducting technology maturity and technical risk assessments is to inform the project and its stakeholders of potential areas of risk so that they can be managed and treated appropriately, and to inform Government of the technical risks for each of the options in a project when considering capability decisions. The Technical Risk Assessment addresses the following basic questions:

- Is the technology feasible?
- Will the technology mature within the required time frame?
- Are there any technical barriers to integrating the capability, both within the system and into the ADF?
- Is the technology fit for the required purpose?

1.6 This Technical Risk Assessment Handbook (TRAH) supports the DCDH by setting out the framework for identifying, assessing and reporting technical risks. The

TRAH assumes knowledge of the CSLC as set out in the DCDH and describes only those processes and inputs from the DCDH that affect technical risk assessment.

Chapter 2
Technical Risk Assessment in Capability Development

2.1 This chapter describes the role of technical risk assessment in Capability Development and the documents that DSTO develops to support the CSLC. The chapter draws on the DCDH, particularly *Annex C Specialised Areas of Knowledge*. This description is included for completeness and those familiar with the DCDH may pass over this chapter.

Technical risk activities up to First Pass Project Approval

2.2 For each project a DSTO Lead Chief of Division (LCOD) and Project Science and Technology Adviser (PSTA) are appointed by DSTO. The PSTA is a member of the Integrated Project Team (IPT) and is responsible for providing coordinated S&T advice to the project. The PSTA is DSTO's primary point of contact for the project, and in particular is responsible for advising the project on technical risk. The PSTA is responsible for the preparation of the Technical Risk Indicator (TRI) and Technical Risk Assessment (TRA), drawing on expertise from DSTO Divisions and other subject matter experts as necessary. The LCOD is responsible for approving the TRI and the TRA.

2.3 **Technical Risk Indicator**. A TRI provides a high-level identification of the feasibility of the technology to provide the capability being proposed, and any potential areas of significant risk associated with the options being considered in the early stages of the project. The TRI is presented to the Options Review Committee (ORC) for consideration of those options that will be progressed to First Pass. The TRI should consider the proposed system from a capability perspective, discussing both the options being considered for further development and the key systems with which the proposed options will need to interact to deliver the required capability. The TRI can identify any developmental systems or technologies which could be developed in time to meet the proposed schedule, and which could potentially provide greater capability than those options previously identified. The TRI allows the ORC to understand the technical risks and issues with the possible options, and inform the selection of which options should progress to First Pass. The TRI also allows appropriate risk treatment and issue resolution strategies to be put in place as soon as practicable. The TRI is developed by the PSTA and is approved by the relevant LCOD.

2.4 **Technical Risk Assessment.** While the TRI provides an early indication of areas of risk, the TRA provides the detailed assessment of the technical risks and issues[1] associated with each option in the capability proposal. The primary purpose of the TRA is to inform stakeholders of these risks and issues and assist the project in the development of effective risk treatments and issue resolution strategies. At this stage of the CSLC, a significant proportion of the technical risks may relate to insufficient technical information. Actions to obtain the necessary information will be part of the risk treatments pursued following First Pass approval.

[1] Risks arise from uncertainties or events that could happen, while issues are events that have happened or are certain to happen.

2.5 A draft First Pass TRA is prepared by the PSTA at the earliest opportunity following the ORC to identify the potential technical risks and issues and to allow the project to develop appropriate treatment strategies for each identified risk[2] and resolution strategies for any significant issues that have been identified. The risks and issues will be presented to the Capability Development Stakeholder Group (CDSG) for consideration and agreement of the treatment and resolution strategies prior to First Pass consideration. The First Pass TRA is approved by the LCOD prior to consideration of the project by the Capability Development Board (CDB).

2.6 **Technical Risk Certification**. The CDS is required by Government to provide an independent assessment of the level of technical risk presented by a project at each Government consideration — primarily First and Second Pass Project Approval, but also when a submission is made to Government seeking an amended Project Approval, eg a Real Cost Increase for a change in scope. The Technical Risk Certification (TRC) is the CDS's statement on technical risk and issues and uses the TRA as guiding input. Following the CDB, the CDS will review the TRA and develop a draft TRC to inform Defence Capability Committee (DCC) consideration. Following DCC approval, the CDS will refine and approve the TRC for inclusion in the MINSUB/CABSUB as appropriate.

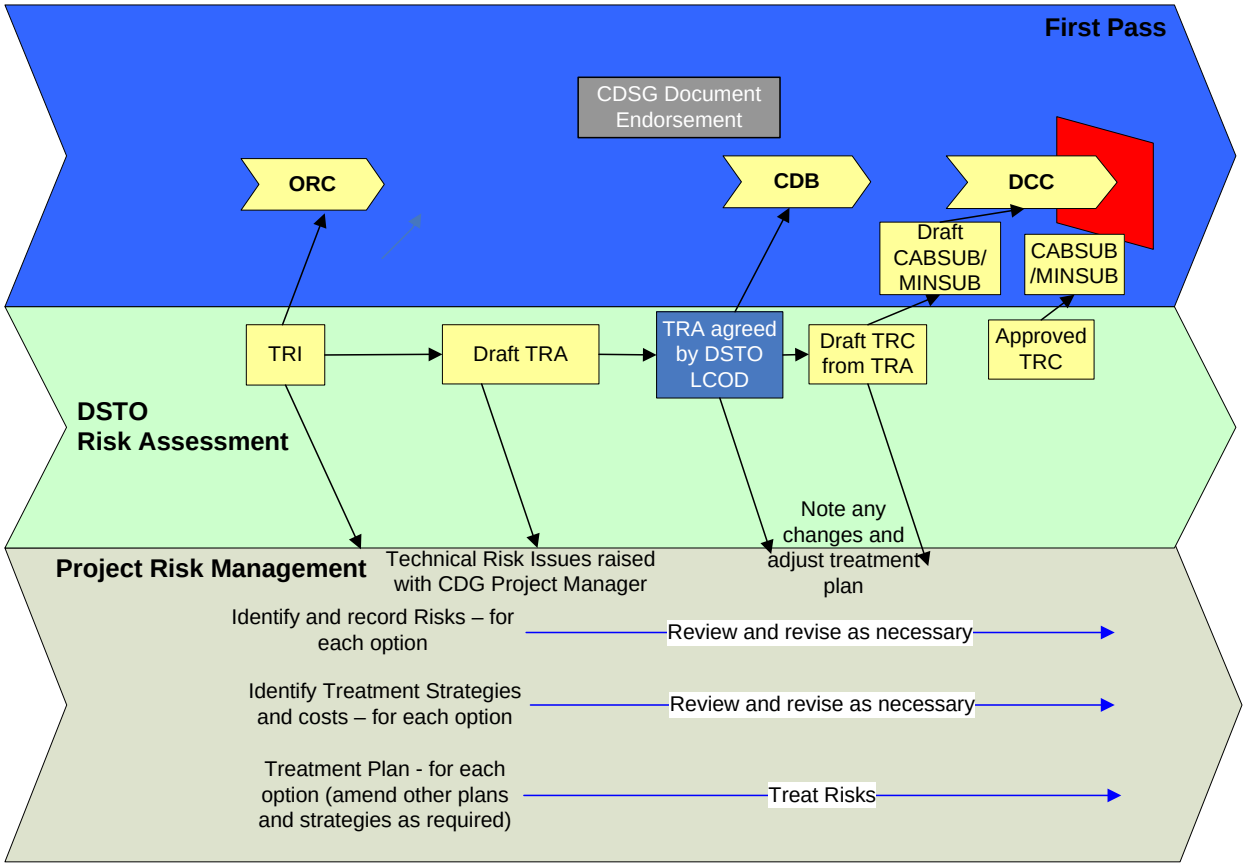

Figure1: Technical risk activities supporting First Pass Project Approval

2.7 Figure 1 summarises the technical risk activities supporting First Pass consideration and Project Approval. Figure 1 also shows how the technical risk

[2] For low risks the default risk treatment is to monitor them.

activities link into project risk management activities as described in the DCDH and in the *DMO Project Risk Management Manual 2010* (PRMM).

Technical risk activities at Intermediate Pass Project Approvals

2.8 If Intermediate Pass Project Approvals are required, the TRA and TRC process will follow a similar path to that described below for Second Pass Project Approval.

Technical risk activities up to Second Pass Project Approval

2.9 Preparation for Second Pass Project Approval focuses on detailed assessment of the options agreed to by Government for further detailed consideration. This assessment will usually require fact-finding and information gathering from appropriate sources facilitated by the project, including Government(s) and industry; the further development of function and performance specifications, particularly those in crucial areas of operational performance; the development of tender documentation; and the evaluation of tender responses. The assessment also includes the identification and execution of risk treatment and issue resolution activities that may involve both DSTO and industry, and the preparation of statements of technical risk.

2.10 **TRA.** Following First Pass approval, the PSTA develops the Second Pass TRA for those options approved for further development at First Pass. The draft Second Pass TRA is regularly updated as any risk treatment activities are completed, up until the document is endorsed by the LCOD for committee consideration. The intent of the Second Pass TRA is to allow Defence to advise Government on the areas and levels of the technical risks and issues associated with the options being proposed for acquisition. Defence will also advise Government on the risk treatment and issue resolution strategies being implemented (such as in the acquisition strategy or through the conduct of trials).

2.11 DSTO may have specific data and information requirements for conducting supporting studies for a project, or it may request through the project that industry deliver specific information to better understand technical risk and develop risk treatment strategies. These requirements for information must be passed to the project to ensure that they are included in the development of documentation that facilitates access to such data, such as a request for proposal or for tender.

2.12 **TRC**. Following the CDB, the CDS will review the approved TRA and develop a draft TRC to inform DCC consideration. Following DCC approval, the CDS will refine and approve the TRC for inclusion in the MINSUB/CABSUB as appropriate.

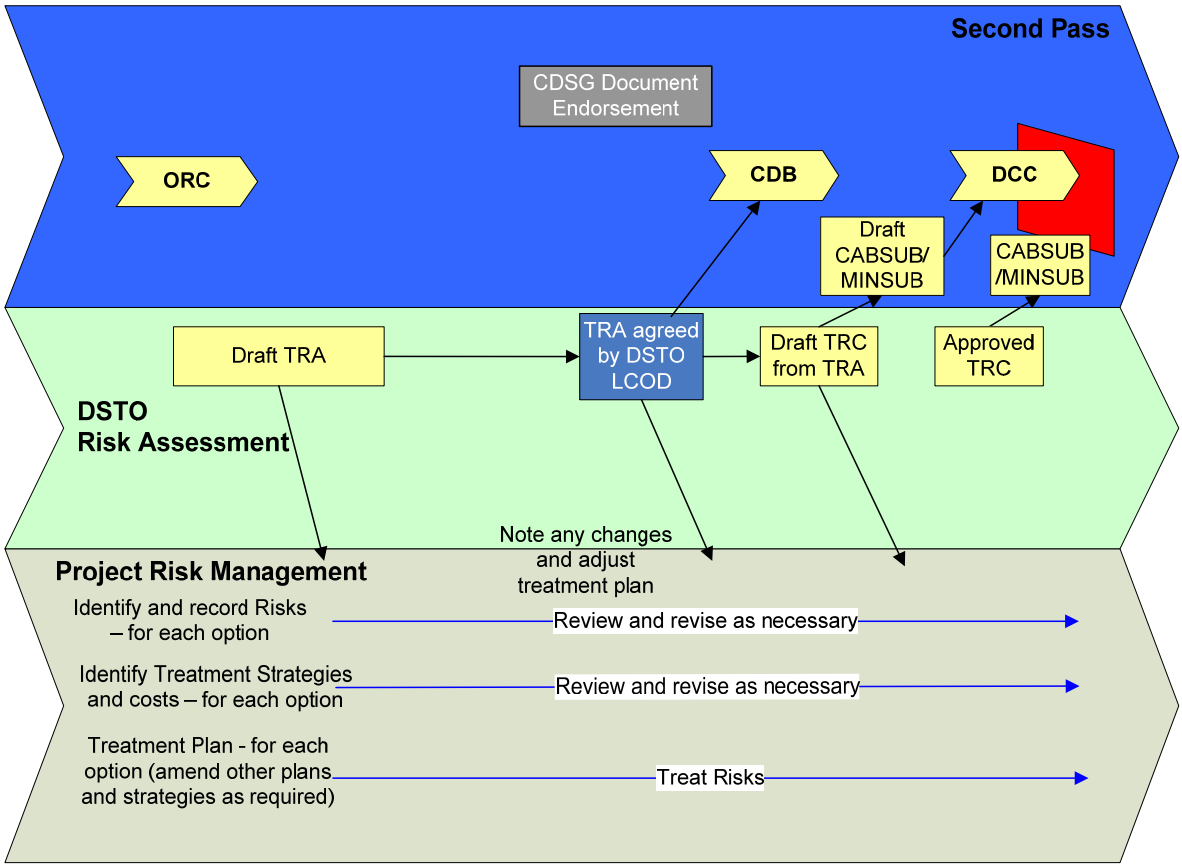

Figure 2: Technical risk activities supporting Second Pass Project Approval

2.13 Figure 2 summarises the technical risk activities supporting Second Pass consideration and Project Approval. Figure 2 also shows how technical risk activities link into the project risk management activities described in the DCDH and in the PRMM.

How technical risk assessment develops

2.14 Technical risk assessment should be seen as an evolving activity of continual review and re-assessment. The requirement of a TRI for ORC, a TRA for First Pass Project Approval and another TRA for Second Pass Project Approval should be viewed as status reports of ongoing risk assessment activities provided at specific milestones of the project.

2.15 The TRI indicates areas of potential technical risk and identifies technical issues. As the First Pass TRA is developed from the TRI, risk events and issues should be developed and assessed, both to allow risk treatment and issue resolution to occur post-First Pass and to inform Government of the technical risks and issues involved in the project. At this early stage in development of the project, the TRA may include a number of sub-systems where the state of maturity of the technology is not known, or where ongoing development is still occurring and it is not possible to assess the risk due to inadequate information. While it is permissible to identify these as unknown risks at First Pass, the intent should be to have these risks assessed by Second Pass.

2.16 Following Government Project Approval, the First Pass TRA becomes the starting point for the draft Second Pass TRA. As information on risk treatments becomes available the draft TRA is regularly updated and re-assessed until it is endorsed for DCC consideration. The Second Pass TRA involves assessing both the current technical risks and the effectiveness of the First Pass risk treatment strategies. Typically at Second Pass there should be few if any unknowns, and if risk treatments have been successful the overall risk level should be lower than at First Pass (although if the risk treatments have not been successful, the risk level may remain the same and indeed could be higher).

How is the technical risk information used?

2.17 Stakeholders in the capability development process use the TRA to understand the level of risk, select appropriate risk treatment strategies and determine the level of contingency. The stakeholders include Defence staff involved in project approval (including CDS, CCDG, the Lead Capability Manager and the acquisition agency's Project Office – typically in the Defence Materiel Organisation (DMO)), staff in other departments who review Defence proposals (such as the Department of Finance and Deregulation and the Department of the Prime Minister & Cabinet), and Ministerial staff. These stakeholders use the TRA for the following purposes:

- to understand the origin and level of technical risk;
- to check that any identified significant technical risks and issues will be managed via appropriate treatment and resolution activities;
- to check that the project strategy and resources are appropriate to the level and type of technical risks and identified issues; and
- CDS uses the TRA as a key input into the TRC provided to Government.

2.18 The project is responsible for project risk management and will incorporate the agreed treatment activities into the Project Management Plan and the Project Risk Management Plan.

2.19 The TRA should not assume that the stakeholders are knowledgeable in the capability or in the specific technical areas covered by the TRA. Therefore, the TRA should provide adequate background and describe technologies and technical risks and issues in a way that is understandable by decision-makers.

Chapter 3
Fundamentals of Technical Risk Assessment

Introduction

3.1 The TRA process is an application of the risk assessment component of the risk and issues management process to the technical risks in major projects. The TRA presents an assessment of the technology maturity levels and the technical risks and issues associated with the project options in an operational capability context. The objective of the TRA is to ensure decision-makers are aware of the technical risks and issues when considering capability options.

3.2 This does not mean that high risk options will not be selected for potential acquisition; rather, the process enables Defence to make informed choices in managing technical risks, and allows identification of capabilities that may present higher levels of risk but also deliver higher payoffs.

Risk assessment

3.3 The process and procedures for assessing technical risk are structured and based on the Australian standards for risk management[3]. The standard defines risk as *'the effect of uncertainty on objectives'* and notes that *'risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence'.* The standard further defines risk assessment as *'the overall process of risk identification, risk analysis and risk evaluation'* and risk management as the *'coordinated activities to direct and control an organisation with regard to risk'*.

3.4 Risk management thus consists of defining the system context, conducting a risk assessment and then treating the risks, as illustrated in Figure 3 which is based on the Australian standard.

3.5 The approach for technical risk assessment follows the risk assessment component of the risk management process shown in Figure 3, and considers those risk sources that are technical in nature. While DSTO is responsible for the development of the TRA for a project and can propose risk treatment strategies, the project is responsible for the overall risk management.

[3] Standards Australia (2009) *Risk management - Principles and guidelines,* AS/NZS ISO 31000:2009

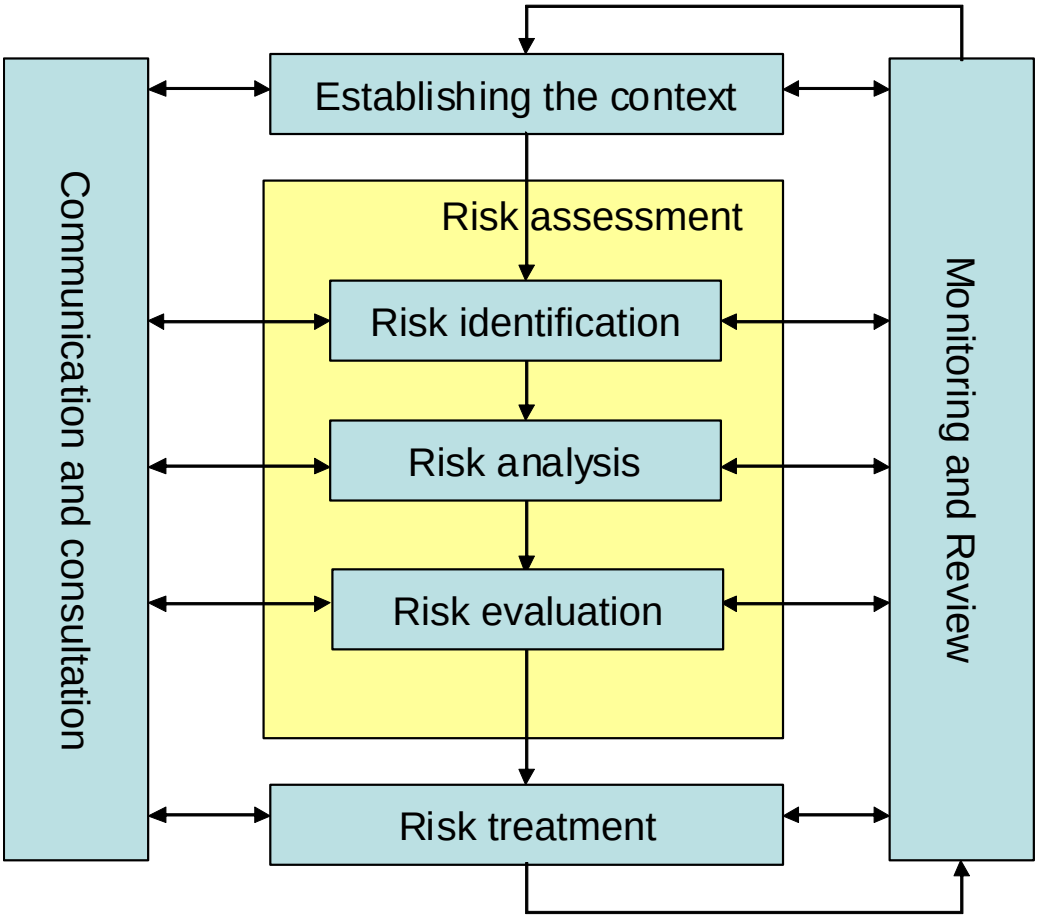

Figure 3: Risk management process

Basis for assessing risk

3.6 As defined in the AS/NZS ISO 31000:2009 standard, risk is the effect of uncertainty on objectives. The *DMO Project Risk Management Manual 2010* (PRMM) states that the Government considers that a successful project is:

> *'a project that delivers a fit-for-purpose capability, as approved by Government, within the approved budget and schedule'* .

3.7 'Fit for purpose' according to the PRMM means that the delivered system is capable of conducting the missions required of it over its expected life. This includes the mission system and support system, cross-system design characteristics such as supportability, and support arrangements such as Australian Industry Involvement.

3.8 To ensure a successful project, the project sets objectives for performance, supportability, safety, cost and schedule which must be met (as defined in the PRMM). Accordingly the technical risk assessment must be made against the objectives of the project. Further, the technical risk is assessed against the proposal for which approval is sought; that is the option set being presented to Government.

3.9 The overall context and scope for a project is defined by the Preliminary Operational Concept Document (POCD) at First Pass and by the Operational Concept Document (OCD) at Second Pass. The required capability or performance

is set out in the Preliminary Function and Performance Specification (PFPS) at First Pass and the Function and Performance Specification (FPS) at Second Pass. The required schedule and estimated costs are described in the Initial Business Case for each option at First Pass and the Acquisition Business Case for each option at Second Pass.

3.10 The PFPS and FPS indicate the capability requirements as essential, important or desirable. The essential requirements define for Government the minimum capability that Defence commits to deliver within the approved budget and schedule. Important and desirable requirements may be traded away during tender negotiations.

3.11 Accordingly, the TRA should focus on the essential project requirements and the ability to meet those and deliver the required performance in time and on budget. Generally, technical risks identified for important and desirable criteria will contribute significantly less to the overall project technical risk. However, there may still be instances where it is necessary to consider important and even desirable criteria, as well as the essential ones, so as to fully consider the technical risks to the project.

Fitness-for-Purpose issues

3.12 From the definition of risk, there has to be uncertainty for a risk to exist. If there is no uncertainty then it is an issue, not a risk[4]. Issues are effects that have happened or will certainly happen[5,6]. Technical issues that prevent the capability option achieving the objectives of the project are termed fitness-for-purpose issues.

3.13 Consider for example a thermal imaging device designed to work effectively in northern Europe. This device is not suitable for use in a tropical rain-forest environment, where the high moisture content of the air leads to strong absorption of infra-red radiation in the frequency bands used by this device. As a result such a device would not be able to effectively detect objects in our environment. This is not a risk as the deficiency is certain, instead it is a technical fitness-for-purpose issue as the device can not provide the capability required.

3.14 Technical fitness-for-purpose issues may arise from technologies and sub-systems that are mature but which have not been demonstrated in the required operating environment. The TRA process will identify these technologies and sub-systems but will not identify if there is an issue involved: this requires further technical analysis and/or performance assessment. Technical issues may also be identified when assessing whether or not the PFPS or FPS can be achieved by the option being assessed. Although issues are identified separately in the TRA, activities introduced to treat a fitness-for-purpose issue may themselves introduce risk. For example, if a piece of equipment is required to fit in a vehicle and one option does not fit, then the choices are to either reject the option or to modify it: but

[4] Shepherd, B. (2003). Managing Risk in a Program Office Environment. Acquisition Review Quarterly, Spring 2003, p125-138.
[5] US Department of Defense (2006). *Risk Management Guide for DOD Acquisition*. Sixth Edition (Version 1.0).
[6] UK Acquisition Operating Framework at http://www.aof.mod.uk/aofcontent/tactical/risk/content/intro.htm

modifying the equipment may introduce a risk, as further development or integration work may be required.

3.15 Fitness-for-purpose issues are described in a specific section of the TRA document. Importantly, because issues are separate from risks, they do not affect the overall level of technical risk.

Technical risk sources

3.16 There are many potential sources of risk to a project, both internal and external, as illustrated in Figure 4 (Figure 4 is not a comprehensive list of all risk sources). The TRA addresses risks that arise from technical sources, both internally and externally sources.

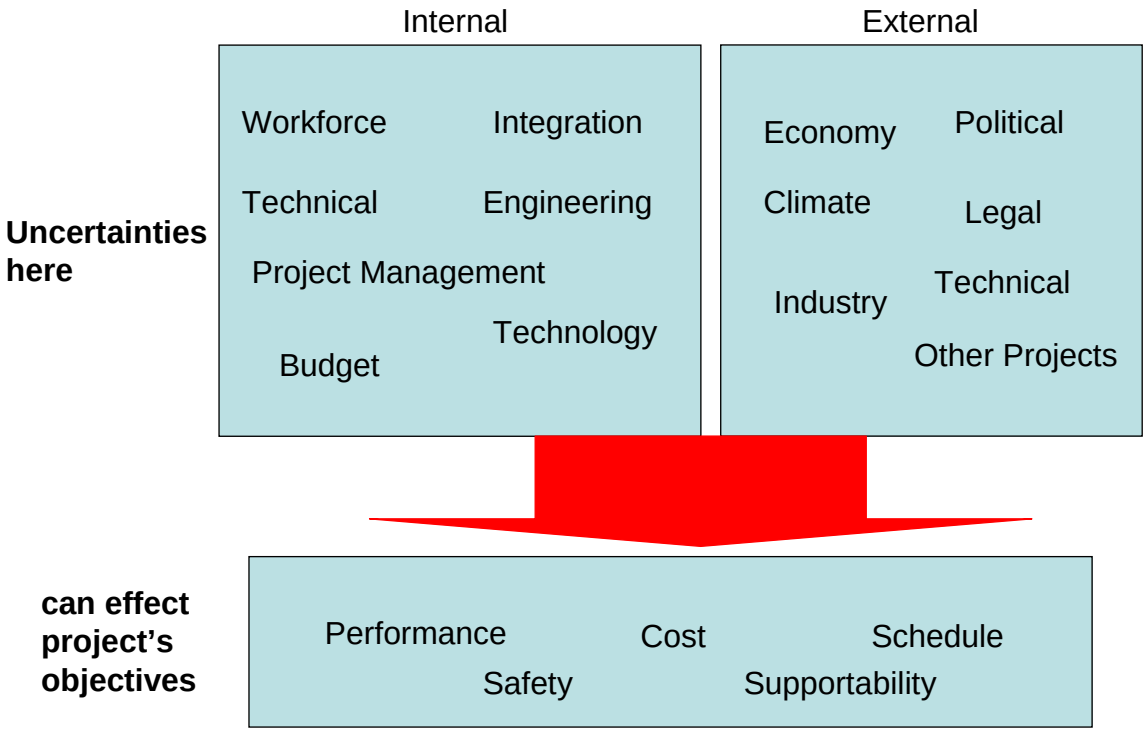

Figure 4: Sources of risk

3.17 There are two broad types of risk that arise from technical sources:

- For a technology that is still being developed there is a likelihood that the technology will not be developed in the time and funding available. This could lead to a potential impact on the required performance, cost and/or schedule. This is termed a technology risk.
- If the sub-systems are still being developed and have not been integrated and demonstrated in the system sought or the system into the ADF, there is the likelihood that the system will not achieve the level of performance required. This could lead to a potential impact on the required performance, cost and/or schedule. This results in a technical risk.

3.18 Technology risk and technical risk are therefore defined as[7]:

Technology risk: **'***the risk that the project will not achieve its objectives due to an underpinning technology not maturing in the required timeframe'.*

Technical risk: *'the risk that the project will not achieve its objectives due to risks which arise in the integration of critical technologies, and/or sub-systems dependent on them, or to the integration of the system into the ADF'.*

3.19 The AS/NZS ISO 31000:2009 standard notes that impacts can be either negative or positive, the later commonly being referred to as opportunities. Technology opportunities are most likely to lead to greater performance than anticipated or delivery earlier than required. Where there are significant opportunities that warrant consideration by the project they should be raised in the TRA.

3.20 The TRA addresses sources of risk that arise only from technical and technology sources, while risks from other source types are assessed by other contributors to the project and integrated into the project risk management plan (eg, workforce risk, cost and schedule risks are all addressed in other risk assessments).

Assessing technical risks

3.21 Technical risks are assessed using a likelihood and consequence framework consistent with the ANS/NZS ISO 31000:2009 standard[8]. In this construct, risks are described through a risk statement that identifies the risk source and the event that could impact on the project's objectives, and describes this impact. Risk statements can be expressed simply as IF…….THEN ……. statements such as:

'IF this risk event were to occur THEN it would impact on achieving one or more project objectives.'

So for example:

'IF the development of the radar is not successfully achieved, THEN this could adversely affect the ability to detect approaching air threats by the required range.'

3.22 More methodically, the risk statement can be expressed in the following form:

'There is a chance that { Project xx…} will be affected by {…risk event…} leading to an impact on {… list of project objectives…}.'

Or for the example above:

'There is a chance that the radar development will not be successful leading to an impact on the required ability to detect approaching air threats by the required range. '

3.23 Risk statements constructed in this latter form help ensure that the risk is clearly described, characterised at the appropriate level to drive management action, and

[7] These definitions have been updated from Moon, T., Smith J., Nicholson J., Fewell, S. and Duus, A. (2004). TRA Principles, Process and Practice. DSTO-GD-0405, to refer to the project's objectives.

[8] Standards Australia (2009) *Risk management - Principles and guidelines,* AS/NZS ISO 31000:2009

linked to the key objectives of the project. A risk event can affect more than one objective and it is important to consider and list all objectives that are impacted. The risk assessment should be based on the highest impact where multiple objectives are impacted by a particular risk.

Risk criteria

3.24 Risk criteria are used to evaluate the significance of risk. The AS/NZS ISO 31000:2009 standard[9] notes that risk criteria should be adapted to meet the objectives of the organisation and of the risk assessment.

3.25 The following risk criteria have been developed to meet Defence's requirements of the TRA, that is, to identify technical risks and issues for risk treatment and issue resolution, and to inform Government of the level of technical risk in a major project[10]. In some circumstances the PSTA may consider that it may be appropriate to adopt different risk criteria, such as for a highly-developmental project or for a project with significant safety risks. In those cases the PSTA may develop appropriate risk criteria in consultation with the Studies Guidance Group (SGG) of DSTO Projects and Requirements Division, who are responsible for technical risk policy and process in DSTO.

3.26 As part of the risk assessment, each risk event identified is examined to estimate the likelihood of its occurrence and its impact on the project's objectives to arrive at the risk itself. Any risk event which is assessed as having a likelihood greater than 50% is rated as ***More Than Likely***, between 20-50% as ***Less Than Likely,*** and less than 20% as ***Unlikely***.

3.27 Once the likelihood is assessed, each risk event is examined to assess the impact of the event, if it were to occur, on the project's objectives in terms of the required performance, supportability, safety, cost or schedule. The impact or consequence is expressed in terms of either ***Major, Moderate or Minor*** as follows:

- **Major:** significant impact on achieving the project's objectives, such as a significant reduction in performance or safety or a major shortfall in supportability.
- **Moderate:** moderate impact on achieving the project's objectives.
- **Minor:** little impact on achieving the project's objectives.

3.28 Once the likelihood and impact for an event are determined, the risk assessment is expressed in terms of high (shown in Table 1 as red), medium (yellow) or low (green) as shown in the risk matrix at Table 1.

[9] Standards Australia (2009) *Risk management - Principles and guidelines,* AS/NZS ISO 31000:2009

[10] Moon, T., Smith, J. and Cook, S.C. (2005). Technology Readiness and Technical Risk Assessment for the Australian Defence Organisation. In *Proceedings of the Systems Engineering, Test & Evaluation Conference, SETE 2005 – A Decade of Growth and Beyond*, Brisbane, Queensland.

Likelihood	Consequence/Impact		
	Minor	Moderate	Major
More Than Likely	MEDIUM	HIGH	HIGH
Less Than Likely	LOW	MEDIUM	HIGH
Unlikely	LOW	LOW	MEDIUM

Table 1: TRA Likelihood/Impact Matrix

3.29 The range of technical risks is the risk profile for the project. The overall technical risk for the project as a whole should be based on a the technical risk profile, and should be assessed in terms of being ***high, medium*** or ***low*** as follows:

- **High:** the technical risk profile is such that there is significant risk to achieving the project's objectives;
- **Medium:** the technical risk profile could lead to a reasonable risk to achieving the project's objectives; and
- **Low:** the technical risk profile is such that there is little risk to achieving the project's objectives.

3.30 The approach described here has been tailored to informing decision-makers of the technical risks and issues in making capability decisions and to informing decisions on the management of those risks and issues.

The use of Readiness Levels in assessing technical risk

3.31 Technology risks arise from technologies that may not be fully developed in the time required, that is from technology immaturity. Technical risks on the other hand arise from systems that may not deliver the performance required due to technology risk or that may not be integrated into the capability or into the ADF in time, either as a consequence of technology immaturity or as a result of sub-system immaturity. The first step in assessing these risks is evaluating the maturity of the technologies and of the systems. Readiness Levels provide a standardised means to measuring this maturity.

3.32 **Technology Readiness Levels (TRL)** are used to describe the maturity of the technologies. TRLs are a 9-point scale first established by NASA for the US space program. TRLs were subsequently used by the US Department of Defense (DoD)[11] and UK Ministry of Defence (MOD)[12] to describe the maturity of technologies being developed for acquisition projects. The TRL of a technology is based on an assessment of the degree to which the technology has been demonstrated or used, as detailed in Table 2.

[11] Office of the Director, Defense Research and Engineering (2009). Technology Readiness Assessment (TRA) Deskbook, July 2009. Prepared by the Director, Research Directorate (DRD).
[12] http://www.aof.mod.uk/aofcontent/tactical/techman/content/trl_whatarethey.htm

Technology Readiness Description	Readiness Level
Basic principles of technology observed and reported.	**1**
Technology concept and/or application formulated.	**2**
Analytical and laboratory studies to validate analytical predictions.	**3**
Component and / or basic sub-system technology validated in a laboratory environment.	**4**
Component and / or basic sub-system technology validated in a relevant environment.	**5**
System sub-system technology model or prototype demonstration in a relevant environment.	**6**
System technology prototype demonstration in an operational environment.	**7**
System technology qualified through test and demonstration.	**8**
System technology qualified through successful mission operations.	**9**

Table 2: Definition of Technology Readiness Levels.

3.33 As shown in Table 2, the lower the TRL the lower the technical maturity. A technology becomes a source of risk if there is a likelihood that the technology will not reach TRL 9 in time to meet the required in-service date. This likelihood is based on expert assessment and may include considerations such as[13]:

- Are the technical requirements known?
- What are the time and resources available?
- What is the level of difficulty in maturing the technology? Is this an extension of previously developed technology or is it leading edge technology?
- Does the system use new technology or components that have never been produced in a factory environment?
- Is a new manufacturing process or technique involved?
- What is the availability of technology expertise? Do the developers have expertise in this area? Have the developers done similar development in the past?
- Does a particular technology represent a scale-up or scale-down that has never been achieved (power density, number of sensors, etc)?
- Are there new materials being used?

3.34 Similarly, **System Readiness Levels (SRL)** are used to describe the maturity of the systems and their integration. The concept of SRLs was introduced by the UK MOD[14] to overcome the limitations of TRLs, which do not address systems

[13] Some of these considerations are drawn from discussion in Arena, M.V., Younossi, O., Galway, L.A., Fox, B., Graser, J.C., Sollinger, J.M., Wu, F. and Wong, C. (2006). Impossible Certainty: Cost Risk Analysis for Air Force Systems. RAND MG-415, 2006.

[14] http://www.aof.mod.uk/aofcontent/tactical/techman/content/srl_whatarethey.htm

integration or whether the technology will result in successful development of the system[15]. DSTO has extended the descriptions of TRLs to SRLs, as shown in Table 3, to describe the technical and integration readiness[16] for the purpose of technical risk assessment.

System Readiness Description	Readiness Level
Basic principles observed and reported.	**1**
System concept and/or application formulated.	**2**
Analytical studies and experimentation on system elements.	**3**
Sub-system components integrated in a laboratory environment.	**4**
System tested in a simulated environment.	**5**
System demonstrated in a simulated operational environment, including interaction with simulations of external systems.	**6**
Demonstration of system prototype in an operational environment, including interaction with external systems.	**7**
System proven to work in the operational environment, including integration with external systems.	**8**
Application of the system under operational mission conditions.	**9**

Table 3: Definition of Systems Readiness Levels

3.35 Some considerations in assessing whether the sub-systems will reach SRL 8/9 and be integrated into the system in time are:

- Does the system represent a new integration of standard sub-systems or integration of yet to be developed sub-systems?
- What is the level of difficulty in maturing each sub-system? Is this an extension of a previously developed sub-system or does it depend upon the development of a new sub-system (in which case there would be an associated technology risk)?
- Does the program use new components that have to be developed or that have never been produced in a factory environment?
- What is the availability of integration expertise? Do the developers have expertise in this area? Have the developers done similar development in the past?

[15] Sauser, B., Ramirez-Marquez, J.E., Magnaye, R., and Tan, W. (2009). A Systems Approach to Expanding the Technology Readiness Level within Defense Acquisition. Int J. Def. Acq. Mgmt., Vol1, p39-58.

[16] Moon, T., Smith, J., and Cook, S.C. (2005). Technology Readiness and Technical Risk Assessment for the Australian Defence Organisation. In *Proceedings of the Systems Engineering, Test & Evaluation Conference, SETE 2005 – A Decade of Growth and Beyond*, Brisbane, Queensland.

3.36 Annex C provides a more detailed description of TRLs for hardware and software, taken from the US DoD Technology Readiness Assessment Deskbook[17] which also provides further information on TRLs and their use, and for SRLs. Further information on TRLs and on SRLs is also available from the UK Acquisition Operating Framework[18,19].

Capability option types

3.37 The DCDH describes the following three types of capability options:

- **Off-the-Shelf options (OTS).** OTS is a system or equipment that: is already established in service; is currently in production and requires only minor modifications to deliver interoperability with the ADF; or is in service with one or more customers for the equivalent purpose. OTS options may be either military (MOTS) or commercial (COTS).
- **Modified Off-the-Shelf options (MOD-OTS).** Modified ('Australianised' or customised) OTS options may be put forward with modifications proposed to meet the particular requirements of the Australian and regional physical environments and/or the ADF's particular operational requirements.
- **Developmental options.** Developmental options pose alternatives where a significantly better outcome and/or technological warfighting advantage may be gained.

3.38 Each capability option type has its own inherent risk profile that will shape the TRI and TRA.

[17] Office of the Director, Defense Research and Engineering (2009). Technology Readiness Assessment (TRA) Deskbook, July 2009. Prepared by the Director, Research Directorate (DRD). Available from https://acc.dau.mil/CommunityBrowser.aspx?id=322190&lang=en-US
[18] http://www.aof.mod.uk/aofcontent/tactical/techman/content/trl_whatarethey.htm
[19] http://www.aof.mod.uk/aofcontent/tactical/techman/content/srl_whatarethey.htm

Chapter 4
Developing the Technical Risk Indicator

Introduction

4.1 The TRI informs ORC consideration of the option set to be developed for First Pass. The TRI identifies areas where the technologies are not sufficiently mature and which are likely to need risk treatment. While the TRI is not a formal risk assessment as there is unlikely to be the depth of information needed at this early stage, the TRI requires a structured process to ensure it supports the subsequent development of the First Pass TRA. As such, the TRI uses the process of considering system boundaries, identifying key technologies and the maturity of those technologies and systems. The final step is to identify those areas where there is the potential for a significant risk. A potential significant risk is one that could require risk treatment (other than just monitoring). The nature of the project (eg, scale and complexity) will have an effect on the structure of the TRI, and particularly whether the proposed option set considers MOTS/COTS options only, or includes modified or developmental options.

4.2 The TRI should identify the project's overall context, its assumptions and objectives from the Project Guidance developed by the project for the ORC, including:

- the capability options being considered;
- the capability system boundaries; and
- the other ADO systems which the capability will need to operate with and whether any of those systems are in development or acquisition.

4.3 For COTS/MOTS options, the TRI should identify:

- any potential significant risks in operating or certifying the option for use in the proposed operating concept and environment; and
- the technologies in the options that are not fit for the purpose proposed.

4.4 For Modified OTS options, the TRI should further identify:

- the sub-systems that are to be adapted or upgraded and the nature of the modifications;
- whether there are any potential significant risks in these modifications; and
- whether there might be any potential significant integration issues arising from the modification.

4.5 For Developmental options**,** the TRI should identify:

- the maturity of the technologies of the key subsystems;
- any potential significant technical risks in developing this option;
- any potential significant integration risks for the system; and
- any potential risk treatment strategies available.

4.6 The TRI can also comment on the fitness-for-purpose of the options, such as the suitability of the technology to meet the project's objectives in the operational environment, or the feasibility of the technology to achieve the project's objectives.

4.7 Risk treatment strategies for developmental or modified OTS options can be suggested, including the potential use of the Capability and Technology Demonstrator program or advice from the Rapid Prototyping, Development and Evaluation Program.

4.8 Finally, the TRI may also raise any technology that is being developed and which could potentially provide an option with enhanced capability or reduced cost and which could be realised in the time available. In particular if there is an option that provides a better course of action, compared to those currently being undertaken or planned, that option should be raised.

TRI structure

4.9 An indicative structure of a TRI is shown in Annex A.

Chapter 5
Developing the Technical Risk Assessment

Introduction

5.1 Most military capabilities are an amalgam of sub-systems and their underlying technologies. For this reason, the TRA process has five stages:

Step 1: Establish the context of use and the project objectives.

Step 2: Identify the sub-systems of the capability.

Step 3: For each sub-system, identify the key underlying technologies, their maturity (via TRLs), the likelihood that the technology will not mature in the time required by the project, the impact on the project's objectives if the technology does not mature or achieve full potential, and hence the technology risks.

Step 4: Consider the integration of the sub-systems and the system (via SRLs), and identify the key technical risk sources in making the sub-systems and system function as an integrated whole, and then assess the likelihood that the sub-systems or system will not be integrated in time, the impact on the project's objectives, and hence the technical risks.

Step 5: With the technology and system level risks identified, make an assessment of the overall level of technical risk to the project.

Step 1 - Establish the context of use

5.2 The first step in risk assessment is to establish the context of use in such a way as to support the assessment of the technical risks. This will be based on the ADF requirement for use of the system as set out in the project's objectives. This should identify the capability sought, the assumptions involved, and the missions required to be performed.

5.3 At project inception, the context of use is the statement of capability need. At the start of a project the Project Guidance from the ORC provides the essential criteria and the Initial Operational Capability and Final Operational Capability. As the project develops further, the development and refinement of the POCD and PFPS at First Pass, and of the OCD and FPS at Second Pass, will provide a detailed context of use that will in turn provide the necessary background information and permit an increasingly refined assessment of the technical risks for the project. The context for use includes the missions that the capability is required to perform, the level of performance required, what other current and future ADF units and systems that this capability needs to work with to achieve those missions, and its supportability over its required life.

5.4 **Establish the system boundaries.** The system boundaries are established from the context of use for the project. It is important to define what is being acquired

in this project, what is not included in the system, and which other Defence systems this capability will need to operate with.

5.5 **External context.** The external context is the external environment in which the capability to be acquired will operate. The external context can include:

- the legal, regulatory, geophysical and climatic environments, spectrum management; and
- other systems that the capability will operate with, including weapon systems, current ADF systems, future ADF systems being acquired through major projects, data links, communication flows, standards etc.

5.6 **Identify objects which pass across boundaries.** Include any objects (including information and data) which flow into and out of the system, their nature and how they may change or be changed by the system. This will help identify the dependencies of the proposed capability on other systems. Examples might include the provision of data from off-board targeting and command and control assets; or weapons, logistic supplies, training or communications bearers not included in the scope of the project.

5.7 Once the dependencies have been identified, an analysis of the project requirements can be conducted. This analysis should ensure that requirements that address any significant interactions with the external environment such as for interoperability with other ADF systems have been explicitly identified.

5.8 The TRA should also identify the dependencies upon other projects as these may be a source of risk. For example, consider a project acquiring a new weapon system for an aircraft that is having its combat system upgraded through another project. If the new weapon can be integrated into the aircraft only if the upgrade is successful, then the risk of the upgrade becomes a risk to the weapon system[20].

Step 2 - Identify the sub-systems

5.9 The capability system being proposed should be broken down into its sub-system elements to guide the understanding and analysis of the underpinning technologies. The PSTA should develop a high-level description of a system and its sub-systems to assist with the subsequent analysis process.

5.10 For example, consider a project acquiring a weapon for an aircraft. The capability comprises the aircraft that will carry and control the weapon, as well as the weapon itself and the aircraft's support systems. Figure 5 depicts the high-level breakdown for this capability, and shows the systems to be acquired by the project in green and the systems that the capability has to interact with in blue[21].

[20] Note that if the weapon is not to be integrated there is no technical risk as there is no dependency.
[21] Note that it is possible to broaden the system further beyond the aircraft if it is deemed appropriate, eg if the weapon is capable of third party targeting, or inclusion of the logistics support system.

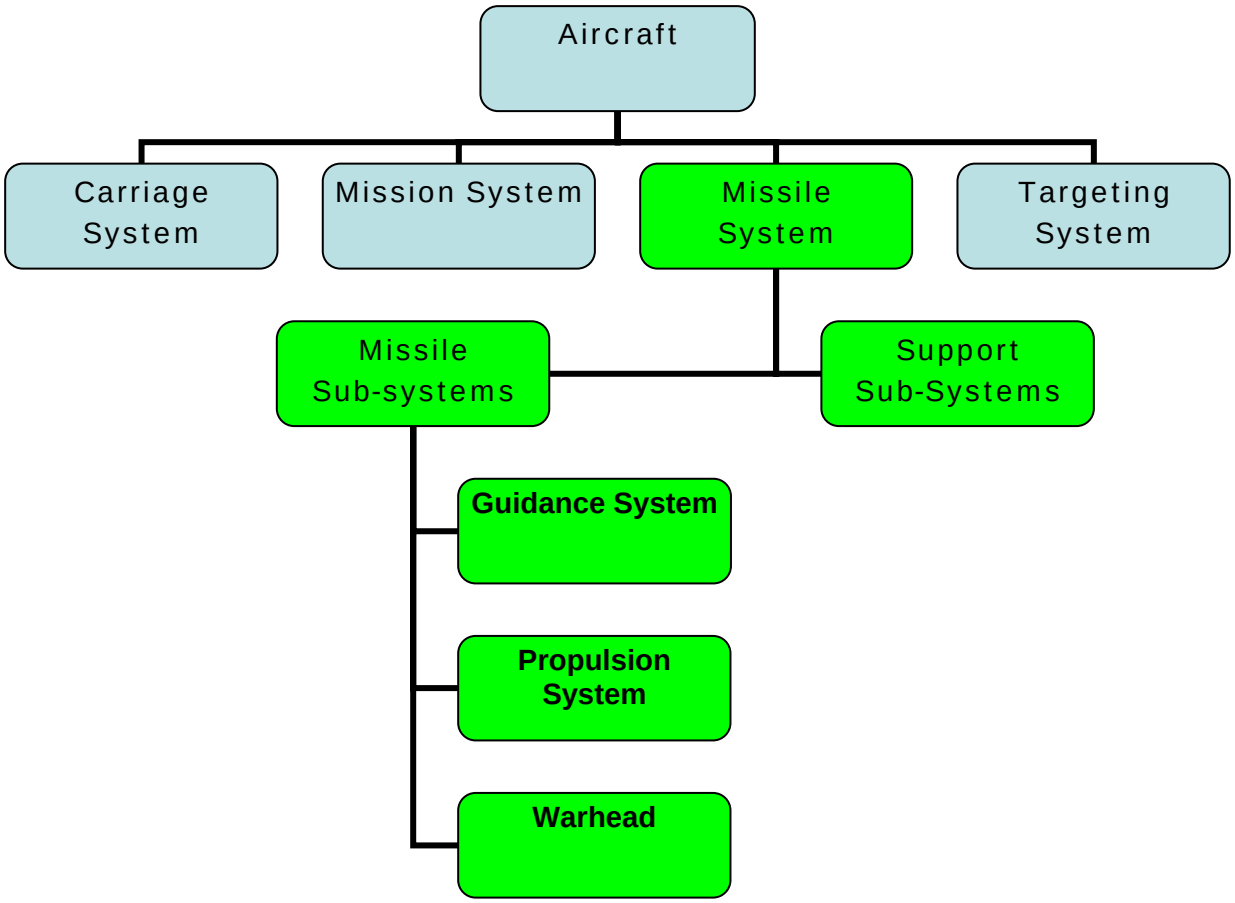

Figure 5: Aircraft weapon system breakdown.

5.11 For an Information and Communication Technology system the sub-systems might include:

- the applications;
- the hardware;
- the human-machine interface; and
- the data links/networking environment.

5.12 While the examples shown here use a system-breakdown approach to identify the underlying technologies, a functional- or process-breakdown can also be used, either instead of the system-breakdown or to supplement it.

5.13 Where a system-breakdown is used, it should be based on the Work Breakdown Structure developed by the project, as set out in the POCD and OCD for First and Second Pass respectively. The system-breakdown can be extended to include areas such as supportability, obsolescence, etc if necessary to address specific technical risk areas. If the options represent different systems or perform different functions, this step may need to be conducted for each of the options.

Step 3 - Assess the technology risks

5.14 Once the sub-systems have been identified, the next step is to identify the technologies that need to be delivered for each sub-system to work. This will lead to

a list for each sub-system of the technologies required to enable that sub-system to work.

5.15 **Evaluate the maturity of each technology**. The TRLs defined in Table 2 form the basis for assessing a technology's maturity. Each contributing technology for each sub-system should be examined to assess its maturity and these assessments should be recorded in the TRA.

5.16 **Identify candidate technology risk events**. If the TRL of a component technology is assessed as 9, then no further development is required. Accordingly this technology is not a source of technology risk, although it can still lead to a technical or integration risk. On the other hand, component technologies that are assessed as TRL less than 9 are potential sources of technology risk. The PSTA should then assess the likelihood that the technology will not be developed to TRL 9 to meet the required in-service date and acquisition schedule, using historical precedence and/or expert judgement. If this is a possibility, then this is a risk source. The likelihood is assessed as either ***More Than Likely***, ***Less Than Likely*** or ***Unlikely,*** as described in paragraph 3.26.

5.17 Once the technology risk sources have been identified, the next activity is to assess the impact on achieving the project's objectives if the risk event were to happen, and hence the level of risk. This leads to a risk statement along the lines of:

> 'There is a chance that the sub-system will not mature sufficiently in the required time, which could impact the project's requirements.'

5.18 These technology risks are then set out using the format at Table 4. As shown in the Table, an estimate of the likelihood can be provided where there is sufficient confidence, either as a point estimate or as a range.

Technology	**TRL**	**Development required**	**Likelihood of technology not maturing in time[1]**	**Impact on project's objectives[2]**	**Risk[3]**
Battery	9	Same battery proven in service on another missile			Nil
Guidance set	5	Shock resistance still to be demonstrated	UNLIKELY (10-15%)	Moderate (Could delay schedule)	Low

Notes.
1. Likelihood is assessed as More Than Likely, Less Than Likely or Unlikely.
2. Impact is assessed as Minor, Moderate or Major.
3. Risk is assessed as Nil, Low, Medium or High.

Table 4: Table of technology risks.

5.19 The Technology Risk table is developed for each option and included as an annex in the TRA. Where the technologies are the same for each option, the risk identification can recorded in the one table.

5.20 A list of considerations that may help identify potential sources of technology risk is in Annex C.

Step 4 - Assess the technical risks

5.21 **Evaluate the maturity of the sub-systems and system as a whole**. The SRLs defined in Table 3 form the basis for assessing a sub-system's maturity. Determining SRLs involves understanding:

- the maturity of each individual technology (TRL);
- the objects that cross the system boundaries;
- the maturity of the process of integrating the component technologies together into the required sub-system; and
- the maturity of the process of integrating the system into the ADF.

5.22 **Identify candidate technical risk events.** For those sub-systems assessed to have an SRL of less than 9, use historical precedent and expert judgement to assess the likelihood that the sub-systems will not mature to SRL 9 in the time available. If this is a possibility, then this is a risk source.

5.23 Once the sub-system risks have been identified, the next activity is to assess the impact from the risk sources on the capability option achieving the project objectives and thence the overall risk level of the event. This assessment requires judgements on:

- how much development is required for this sub-system to meet the requirement;
- estimating the likelihood that the sub-system will not be developed and integrated in the time required; and
- the impact on the project's objectives.

5.24 The level of detail required to accurately evaluate SRLs often only emerges in the response to the tender process, which occurs between First and Second Pass. Additionally further system risks may be identified which were previously unrecognised, while some risks that may have been identified earlier may no longer be relevant, or may have become issues.

5.25 The final activity is to assess the potential impact of the risk sources on the integration and interoperability of the capability option with other ADF capabilities as identified by the project's objectives. This assessment requires judgements on:

- how much development is required for this system to meet the requirements;
- how much development is required for any other systems;
- estimating the likelihood that the system will not be developed and integrated into the ADF in the time required; and
- the impact on the project's objectives.

5.26 The identified technical risk events should be described in sufficient detail so that project staff and other stakeholders are able to understand the underlying technology risks and their level and likelihood, so that the project is able to develop appropriate risk treatment strategies.

5.27 These technical risks are then set out using the format at Table 5. This table is incorporated for each option in an annex in the TRA and the significant technical risks are described in a section in the TRA. For MOTS/COTS solutions with sub-systems with fully mature technologies, the second and third columns can be omitted.

Sub-system	Technologies in each sub-system	TRL	SRL	Integration required	Likelihood of not being integrated in time[1]	Impact on project's objectives[2]	Level of Risk[3]
Guidance System	Battery	9	5	Guidance set to be integrated	Less than likely (30%)	Moderate	**MEDIUM**
	Guidance set	5					
	etc						
etc							
System							
Missile System			7	Integration with aircraft mission system	Less than likely (30-50%)	Major	**HIGH**

Notes.
1. Likelihood is assessed as More Than Likely, Less Than Likely or Unlikely.
2. Impact is assessed as Minor, Moderate or Major.
3. Risk is assessed as Nil, Low, Medium or High.

Table 5: Table of technical risks

5.28 A list of considerations that may help identify potential sources of technical risk is in Annex C.

5.29 The significant risks are reported in the TRA in the format in Table 6. The assessment of whether a risk is significant and should be reported in the TRA will depend upon the risk level, the likelihood and impact, and the overall risk profile of the project. It is suggested that the emphasis should be on those risks that should be actively treated (that is other than monitored).

Project Objective	Risk Description	Likelihood	Impact	Risk Level
Ability to detect aircraft up to x km	Radar performance	Less than likely	Moderate	**MEDIUM**
Must be able to carry air-to-surface weapon	Weapon carriage	Less than likely	Moderate	**MEDIUM**
	Certification of new interface	More than likely	Major	**HIGH**

Table 6. Description of significant technical risks in the TRA.

5.30 **Is it a technical risk?** In deciding whether a proposed risk is actually a technical risk the following checklist should be considered:

- Is the source of the risk due to technology immaturity or system integration immaturity?
- Is there uncertainty?
- What further research or development is needed to mature the technology of the sub-system or the integration of the system?
- Can the risk be treated primarily through programmatic means, eg changes to the work breakdown, tasks/activities and schedule logic? If so it is unlikely to be a technical risk.

5.31 **Dealing with unknowns**. Assessing technical risks is inherently about dealing with uncertainty. However, in some cases there may be no knowledge at all of a sub-system, making it difficult to undertake an assessment. For example, the project may not have made a selection of the electronic warfare (EW) system for a platform and the risk is that the EW system will not be integrated into the combat system in time. While the draft TRA is being developed, these potential risk events can be described as unknown in order to flag that risk treatment is required, namely to obtain the necessary information to enable a complete assessment to be conducted. For the endorsed TRA and particularly for the Second Pass TRA, it is desirable to provide a more useful assessment than unknown.

5.32 There are two practical approaches to handling a shortfall of information:

- **Either** assume that the risk event is more than likely to occur, and then assess the impact and hence the risk. Thus risk events which have major or moderate impact on project outcomes will be assessed as high risk, while risk events that have minor impact can be assessed as medium. This is a worst-case assessment.
- **Or** consider the range of possible options and assess whether the risks are different across the range. So in the example of an EW system for a platform, it might be possible to assess for those EW systems that have already been integrated into the combat system that the technical risk is low, while for those other options which have not already been integrated into the combat system the risk might be high.

Step 5 - Determining overall risk level

5.33 The risk profile can be summarised using either the format at Table 7 or at Table 8. The Tables include the overall technical risk level as defined in paragraph 3.29.

Project AIR 1234 TRA Summary			
Likelihood	**Consequence/Impact**		
	Minor	**Moderate**	**Major**
More Than Likely		**Radar development**	**Corrosion control**
Less Than Likely	**Weapon integration**	**Engine development, blast protection**	
Unlikely	**Airframe development**		
Overall Technical Risk Level	**HIGH**		

Table 7: The risk profile as a matrix.

Project AIR 1234 TRA Summary			
Risk Event Title	**Likelihood**	**Impact**	**Risk Level**
Radar performance	**Less than likely**	**Moderate**	**MEDIUM**
Weapon carriage	**Less than likely**	**Moderate**	**MEDIUM**
Certification	**More than likely**	**Minor**	**HIGH**
Corrosion control	**Unlikely**	**Moderate**	**LOW**
Overall Technical Risk Level	**MEDIUM**		

Table 8: Table form of the risk profile.

5.34 Analysis of the risk profile matrix will often allow a judgement on the overall level of technical risk. For large complex projects it may be difficult and indeed potentially misleading to provide a 'one-word' overall risk assessment. In these cases it is reasonable to provide summary risk levels for the key systems. For example, a project procuring a new ship may present significant risks in the areas of hull form, propulsion, electronic systems and weapon systems.

Technology and Technical risks in MOTS/COTS options

5.35 Where an option is completely OTS, all the technologies and sub-systems have been integrated and demonstrated, although not necessarily in the operational mission conditions. That is the TRLs should all be 9, and some or all of the SRLs

could be less than 9. As a result, there should be no technology risks because the technologies are mature but technical risks are possible. However, in practice few MOTS/COTS systems will have been demonstrated in relevant mission operations and hence may not be TRL 9.

5.36 In conducting the TRA for a MOTS/COTS option it is important to consider carefully whether any technology risks do exist. The existence of technology risks would suggest that the option might not actually be a MOTS/COTS option, as these risks would imply that further development is needed. Thus the PSTA should assess whether or not all the technologies are indeed mature.

5.37 If all the technologies are indeed mature, then there is no need to proceed any further with step 3 of the TRA approach, as there are no technology risks and the assessment can proceed directly to step 4. If, however, there are some technologies that are not mature, then those will need to be assessed for any potential technology risks.

5.38 While there may be no technology risks for a MOTS/COTS option, technical risks can still arise from the following considerations:

- operation and certification in the required environment - will these systems require modification for environment (shock, vibration, electromagnetic, etc)?
- integration and interoperability with other ADF capabilities, including future capabilities;
- the ability of the design to accommodate future upgrades in technology, given the cycle rate for such technology in the commercial sector?
- supporting the option over its planned life-of-type. How long will the manufacturer support and produce the system and sub-systems?

5.39 Some of the more challenging integration risks come from the potentially misleading assumption that disparate MOTS/COTS solutions can be simply integrated together to form a system suitable for use by the ADF.

5.40 A MOTS/COTS option may also have fitness-for-purpose issues, largely because the equipment will have been developed for a lead customer who may have differing requirements, operational concepts, or a different operational environment from the ADO. Thus the OTS option may not meet one or more of the capability requirements, particularly where the option has not been demonstrated in the mission conditions required. The inability to meet a requirement for a technical reason is a fitness-for-purpose issue which should be included in the relevant section of the TRA.

5.41 Accordingly, if assured that all the technologies are indeed mature, the TRA can focus on the potential technical risks in the areas identified above, and on any fitness-for-purpose issues.

Technical risks in Modified OTS

5.42 Where there is an intention to modify an OTS system, technology risks can arise from any development work necessary to make the solution fit the requirement. There may also be technical risks arising from the integration of those sub-systems

being modified. In this case the analysis of technology risks will focus on the sub-systems being modified or developed, while technical risks could arise from the integration of these modified sub-systems into the system as well as the integration and interoperability of the other sub-systems. There may also be fitness-for-purpose issues arising from the mature technologies and sub-systems.

Technical risks in developmental options

5.43 Developmental options require the most comprehensive assessment as there may be many areas of potential technology and technical risks. As well as identifying and assessing these risks, the viability of the risk treatment strategies is a key consideration in whether to proceed with a developmental option.

Technical risk drivers

5.44 In some circumstances where there is a medium or high technical risk, the risk may be driven by a particular requirement, whether a performance requirement or the schedule. For example, a retrieval system from a ship may have been previously demonstrated in sea state 3 whereas the project's requirements may seek a system that can operate in sea state 5 resulting in a need for development and introducing risk. The TRA should identify those areas of technical risk that are most sensitive to the requirements. In many respects this is a sensitivity analysis to identify those technical risk areas that are most sensitive to the project's objectives.

Proposing possible risk treatment strategies

5.45 The TRA may suggest risk treatment strategies for any of the identified risks, and in particular for those HIGH and MEDIUM risks. The TRA should identify any high or medium risks where risk treatment is not identifiable. Where the project has proposed risk treatment strategies the TRA can also comment on the viability or likely effectiveness of those.

5.46 Risk treatment options can include any of the following:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- removing the risk source eg accepting the shortfall;
- undertaking activities to reduce the likelihood;
- undertaking activities to reduce the consequences if the risk were to be realised;
- sharing the risk with another party or parties (including contracts and risk financing);
- retaining or accepting the risk by informed decision; or
- a combination of the above.

5.47 For technical risks, risk treatment strategies generally either reduce the likelihood of a risk eventuating, reduce the impact if the risk does eventuate, or remove the risk source by proposing a lower-risk technical alternative. Typical risk treatment strategies might include:

- system and sub-system demonstration activities to monitor and improve TRLs and SRLs;
- management and contractual measures to encourage suppliers to improve management of technical risk;
- system and sub-system integration test-beds to increase system readiness levels;
- identification of intermediate design reviews and decision points as possible additional risk treatment strategies; or
- the identification of alternative lower-risk technology solutions as fall-back options if a risk eventuates.

5.48 The risk treatment strategies may also need to consider arrangements to monitor contractor progress with technology development or system integration activities, and to seek additional information where confidence in the risk assessment is low.

5.49 As risk treatment can involve test and evaluation of the options or prototypes, the PSTA should consult with the Australian Test and Evaluation Office to ensure that appropriate risk treatments are included in the project's Test Concept Document.

5.50 While the TRA can suggest risk treatment strategies, it is the responsibility of the project to develop the risk treatments. This is because the project must consider risks from many sources other than technical risk, as shown in Figure 4. Accordingly the project must develop risk treatment strategies that best address the range of risk sources and risks. For example, a risk treatment proposed to treat a technical risk might adversely affect a workforce risk if considered in isolation: risk treatment needs to be developed at the project level to reduce both the technical and workforce risks in this case. Selection of appropriate risk treatments will take into account a number of factors including the likely effectiveness of the risk treatments across all risks, the cost of the treatments and any regulatory or environmental issues.

5.51 The risk treatment strategies adopted by the project need to be incorporated into the project risk management plan, in accordance with the DCDH and the PRMM.

Residual risks

5.52 Residual risks are the risks remaining after risk treatment, with the level of residual risk being dependent upon the success of the risk treatment. Residual risks are used to choose between risk treatment strategies, with the most cost-effective strategies being preferred.

5.53 Where possible, the PSTA can assess the likely effectiveness of the identified technical risk mitigation strategies and hence the residual risk to assist the project in selecting risk treatment strategies as noted in para 5.49.

Confidence of assessment

5.54 The confidence in the assessment of the risks and their sensitivity to the assumptions made in the project should be considered. Factors to consider include

the degree of divergence of expert judgements, the uncertainty in making those judgements, any limitations in the data available, and the sensitivities in the assessment to the project requirements. It is likely that the confidence in the assessment will be lower earlier in the development of the project due to the greater inherent uncertainty. The confidence in the assessment should be expressed as high, medium or low.

TRA structure

5.55 The indicative structure of a TRA is shown in Annex B.

Risk analysis methods and expert judgements in TRA

5.56 Risk analysis can use a variety of methods, either qualitative or quantitative, to assess the likelihood and the impact and the overall risk. These methods include fault-tree analysis, Monte Carlo simulation techniques, probabilistic modelling methods and the use of expert judgement[22]. In conducting technical risk assessments, the PSTA should use a technique that is appropriate to the problem. The PSTA should consult experts in these techniques in DSTO. In most cases the method used will use expert judgement due to the lack of historical data.

5.57 While the steps to develop the TRA in this Handbook have been described in terms of using expert judgement as this is the most likely method that will be used, the approach is applicable whatever the risk analysis method is used. However, in using expert judgement the PSTA should be aware of the limitations of experts in assessing subjective probabilities and risks, and should consult relevant experts in DSTO where appropriate.

5.58 Research has shown that human psychology includes various heuristics that can lead to biases in our judgements. These biases tend to make us overconfident when assessing probabilities (that is underestimating the actual probability) and overoptimistic when assessing the risks[23].

5.59 These biases can be reduced in a number of ways, although they cannot be completely avoided. First it has been shown that some biases decrease with domain knowledge. Structured decision-making approaches can be used to encourage experts to think analytically. To improve the accuracy of the judgements, a number of experts can be asked for their judgement to asses what variability there is and their judgements combined. Finally, experts should review all the available information and should explain their reasoning for peer review.

5.60 Within the context of conducting a TRA, the structured approach set out in this Handbook should encourage experts to think analytically. The PSTA responsible for the TRA should ensure they consult with experts in the technologies of relevance to

[22] For example see ISO/IEC 31010:2009 *Risk management – Risk assessment techniques.*

[23] For a recent overview of this area see O'Hagan, A., Buck, C.E., Daneshkhah, A., Eiser, J.R., Garthwaite, P.H., Jenkinson, D.J., Oakley J.E. and Rakow T. (2006) .*Uncertain Judgements: Eliciting Experts' Probabilities*. John Wiley & Sons, Ltd.

the project concerned, as well as experts in risk assessments and experts in subjective probability elicitation. The same panel of experts should be used to assess all the options to ensure a valid comparison. The key consideration is to ensure that the risk assessment process provides constructive insights into the technical risks of the different capability options to support decision-making.

5.61 The PSTA should describe the method used to conduct the risk assessment in the TRA. Where expert judgement has been used, the TRA should identify the experts involved and their area of expertise.

Acronyms

ADF	Australian Defence Force
ADO	Australian Defence Organisation
CABSUB	Cabinet Submission
CDG	Capability Development Group
CDB	Capability Development Board
CDS	Chief Defence Scientist
CDSG	Capability Development Stakeholder Group
CM	Capability Manager
COD	Chief of Division
COTS	Commercial off-the-shelf
CSLC	Capability Systems Life Cycle
DCC	Defence Capability Committee
DCDH	Defence Capability Development Handbook
DMO	Defence Materiel Organisation
DoD	United States Department of Defense
DSTO	Defence Science and Technology Organisation
EW	Electronic Warfare
FPS	Function and Performance Specification
IPT	Integrated Project Team
LCOD	DSTO Lead Chief of Division
MINSUB	Ministerial Submission
MOD	United Kingdom Ministry of Defence
MOD-OTS	Modified off-the-shelf
MOTS	Military off-the-shelf
OCD	Operational Concept Document
ORC	Options Review Committee
OTS	Off the shelf
POCD	Preliminary Operational Concept Document
PFPS	Preliminary Function and Performance Specification
PRMM	Project Risk Management Manual
PSTA	Project Science and Technology Adviser
TRA	Technical Risk Assessment
TRAH	Technical Risk Assessment Handbook
TRC	Technical Risk Certification
TRI	Technical Risk Indicator
TRL	Technology Readiness Level
SGG	Studies Guidance Group
SRL	System Readiness Level

Annex A
Indicative Structure of Technical Risk Indicator

Introduction
Aim of Project
- Overview of project, its objectives and assumptions
- Project dependencies
- Overview of Proposed Options

Potential Technical Risk Areas
- Option 1- describe significant risks from tables in Annex A
- Option 2 etc

Technical Issues
- For options as appropriate

Emerging Technologies & Other Options
- If appropriate

TRI Summary

Annex A. Option 1 Risk Indicator worksheet[1]
Annex B. Option 2 Risk Indicator worksheet[1]
Etc

Note 1: The specific worksheet elements will depend upon on the capability option type, that is whether it is MOTS/COTS, modified OTS or developmental.

Annex B
Indicative Structure of Technical Risk Assessment

Technical Risk Assessment – Executive Summary
Introduction
Aim of Project
- Overview of project, its objectives and assumptions
- Project requirements
- Description of Proposed Options

System Description
- System breakdown & System boundaries
- Technical dependencies on current and future ADF systems

Methodology
- A short description of how the likelihoods and impacts were assessed. Where expert judgement is used this should identify the experts involved and their area of expertise, including experts in risk assessment and subjective knowledge elicitation.

Technology Risks
- Significant areas of technology immaturity and associated risks from Annex A for each option. For Second Pass TRA this could include a description of how risks have changed since First Pass.
- For a MOTS/COTS option there may be no technology risks in which case there may be no need to include that option in this section

Technical Risks
- Significant areas of sub-system immaturity and associated risks from Annex B for each option. For Second Pass TRA this could include a description of how risks have changed since First Pass.

Technical Risk Drivers (if appropriate)
- Are there any areas of technical risk that are particularly sensitive to the project's objectives?

Fitness-for-Purpose Issues
- Technical fitness-for-purpose issues for options as appropriate

Risk Treatment
- Potential risk treatments for key risks

TRA Summary & Conclusion
- Risk Profile
- Key risks & issues for each option
- Overall risk assessment for each option

Annex A. Technology Risk analysis for each applicable option[1]
Annex B. Technical Risk analysis for each option[2]
Etc

Notes:
1. This is the analysis set out in Table 4 in Section 5 of the TRAH.
2. This is the analysis set out in Table 5 in Section 5 of the TRAH.

Annex C
TRL and SRL Descriptions

Hardware Technology Readiness Levels from DoD TRA Deskbook

TRL Definition	Description	Supporting Information
1 Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development (R&D). Examples might include paper studies of a technology's basic properties.	Published research that identifies the principles that underlie this technology. References to who, where, when.
2 Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.	Publications or other references that outline the application being considered and that provide analysis to support the concept.
3 Analytical and experimental critical function and/or characteristic proof of concept.	Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.	Results of laboratory tests performed to measure parameters of interest and comparison to analytical predictions for critical subsystems. References to who, where, and when these tests and com-parisons were performed.
4 Component and/or bread-board validation in a laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared with the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.	System concepts that have been considered and results from testing laboratory-scale breadboard(s). References to who did this work and when. Provide an estimate of how breadboard hardware and test results differ from the expected system goals.
5 Component and/ or breadboard validation in a relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so they can be tested in a simulated environment. Examples include "high-fidelity" laboratory integration of components.	Results from testing a laboratory breadboard system are integrated with other supporting elements in a simulated operational environment. How does the "relevant environment" differ from the expected operational environment? How do the test results compare with expectations? What problems, if any, were encountered? Was the breadboard system refined to more nearly match the expected sys-tem goals?
6 System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment.	Results from laboratory testing of a prototype system that is near the desired configuration in terms of performance, weight, and volume. How did the test environment differ from the operational environment? Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
7 System prototype demonstration in an operational environment.	Prototype near or at planned operational system. Represents a major step up from TRL 6 by requiring demonstration of an actual system prototype in an operational environment (e.g., in an aircraft, in a vehicle, or in space).	Results from testing a prototype system in an operational environment. Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
8 Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation (DT&E) of the system in its intended weapon system to determine if it meets design specifications.	Results of testing the system in its final configuration under the expected range of environmental conditions in which it will be expected to operate. Assessment of whether it will meet its operational requirements. What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before finalizing the design?
9 Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation (OT&E). Examples include using the system under operational mission conditions.	OT&E reports.

Software Technology Readiness Levels from DoD TRA Deskbook

TRL Definition	Description	Supporting Information
1 Basic principles observed and reported.	Lowest level of software technology readiness. A new software domain is being investigated by the basic research community. This level extends to the development of basic use, basic properties of software architecture, mathematical formulations, and general algorithms.	Basic research activities, research articles, peer-reviewed white papers, point papers, early lab model of basic concept may be useful for substantiating the TRL.
2 Technology concept and/or application formulated.	Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies using synthetic data.	Applied research activities, analytic studies, small code units, and papers comparing competing technologies.
3 Analytical and experimental critical function and/or characteristic proof of concept.	Active R&D is initiated. The level at which scientific feasibility is demonstrated through analytical and laboratory studies. This level extends to the development of limited functionality environments to validate critical properties and analytical predictions using non-inte-grated software components and partially representative data.	Algorithms run on a surrogate processor in a laboratory environment, instrumented components operating in a laboratory environment, laboratory results showing validation of critical properties.
4 Module and/or subsystem validation in a laboratory environment (i.e., software prototype development environment).	Basic software components are integrated to establish that they will work together. They are relatively primitive with regard to efficiency and robustness compared with the eventual system. Architecture development initiated to include interoperability, reliability, maintain-ability, extensibility, scalability, and security issues. Emulation with current/legacy elements as appropriate. Prototypes developed to demonstrate different aspects of eventual system.	Advanced technology development, stand-alone prototype solving a synthetic full-scale problem, or standalone prototype processing fully representative data sets.
5 Module and/or subsystem validation in a relevant environment.	Level at which software technology is ready to start integration with existing systems. The prototype implementations conform to target environment/interfaces. Experiments with realistic problems. Simulated interfaces to existing systems. System software architecture established. Algorithms run on a processor(s) with characteristics expected in the operational environment.	System architecture diagram around technology element with critical performance requirements defined. Processor selection analysis, Simulation/Stimulation Laboratory buildup plan. Software placed under configuration management. Commercial-of-the-shelf/government-off-the-shelf components in the system software architecture are identified.
6 Module and/or subsystem validation in a relevant end-to-end environment.	Level at which the engineering feasibility of a software technology is demonstrated. This level extends to laboratory prototype implementations on full-scale realistic problems in which the software technology is partially integrated with existing hardware/software systems.	Results from laboratory testing of a prototype package that is near the desired configuration in terms of performance, including physical, logical, data, and security interfaces. Comparisons between tested environment and operational environment analytically under-stood. Analysis and test measurements quantifying contribution to system-wide requirements such as throughput, scalability, and reliability. Analysis of human-computer (user environment) begun.
7 System proto-type demonstration in an operational high-fidelity environment.	Level at which the program feasibility of a software technology is demonstrated. This level extends to operational environment proto-type implementations, where critical technical risk functionality is available for demonstration and a test in which the software technology is well integrated with operational hardware/software systems.	Critical technological properties are measured against requirements in an operational environment.
8 Actual system completed and mission qualified through test and demonstration in an operational environment.	Level at which a software technology is fully integrated with operational hardware and software systems. Software development documentation is complete. All functionality tested in simulated and operational scenarios.	Published documentation and product technology refresh build schedule. Software resource reserve measured and tracked.
9 Actual system proven through successful mission-proven operational capabilities.	Level at which a software technology is readily repeatable and reusable. The software based on the technology is fully integrated with operational hardware/software systems. All software documentation verified. Successful operational experience. Sustaining software engineering support in place. Actual system.	Production configuration management reports. Technology integrated into a reuse “wizard.”

Additional TRL Definitions from TRA Deskbook

Term	Definition
Breadboard	Integrated components that provide a representation of a system/subsystem and that can be used to determine concept feasibility and to develop technical data. Typically configured for laboratory use to demonstrate the technical principles of immediate interest. May resemble final system/subsystem in function only.
High Fidelity	Addresses form, fit, and function. A high-fidelity laboratory environment would involve testing with equipment that can simulate and validate all system specifications within a laboratory setting.
Low Fidelity	A representative of the component or system that has limited ability to provide anything but first-order information about the end product. Low-fidelity assessments are used to provide trend analysis.
Model	A functional form of a system, generally reduced in scale, near or at operational specification. Models will be sufficiently hardened to allow demonstration of the technical and operational capabilities required of the final system.
Operational Environment	Environment that addresses all the operational requirements and specifications required of the final system to include platform/packaging.
Prototype	A physical or virtual model used to evaluate the technical or manufacturing feasibility or military utility of a particular technology or process, concept, end item, or system.
Relevant Environment	Testing environment that simulates both the most important and most stressing aspects of the operational environment.
Simulated Operational Environment	Either (1) a real environment that can simulate all the operational requirements and specifications required of the final system or (2) a simulated environment that allows for testing of a virtual prototype. Used in either case to determine whether a developmental system meets the operational requirements and specifications of the final system.

The above tables in this Annex are reproduced from the *Technology Readiness Assessment (TRA) Deskbook*, July 2009. Prepared by the Director, Research Directorate (DRD), Office of the Director, Defense Research and Engineering (DDR&E).

System Readiness Levels[1]

SRL Definition	Description
1. Basic principles observed and reported	Lowest level of system readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a system's basic properties.
2. System concept and/or application formulated	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3. Analytical and experimental critical function and/or characteristic proof of concept	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the system. Examples might include COTS components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment	Basic system components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
5. Component and/or breadboard validation in relevant environment	Fidelity of system components increases significantly. The basic system components are integrated with reasonably realistic supporting elements so the total system can be tested in a simulated environment. Examples include "high-fidelity" laboratory integration of components into system elements.
6. System/subsystem model or prototype demonstration in a relevant environment	Representative model or prototype system, which is demonstrated in a well-simulated operational environment, including interaction with simulations of key external systems.
7. System prototype demonstration in an operational environment	Prototype near, or at, planned operational system. Represents a major step up from SRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space, including interaction with external systems.
8. Actual system completed and qualified through test and demonstration	System has been proven to work in its final form and under expected conditions, including integration with external systems. In almost all cases, this SRL represents the end of true system development. Examples include test and evaluation of the system in its intended context and operational architecture to determine if it meets design specifications.
9. Actual system proven through successful mission operations	Actual application of the system in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

1. From 'TRA of Defence Projects - Tiger Team Assessment", J. Smith, G. Egglestone, P. Farr, T. Moon, D. Saunders, P. Shoubridge, K. Thalassoudis and T. Wallace, DSTO-TR-1656, 2004.

Annex D
Potential considerations in Technical Risk Assessment

This section describes some considerations that may help identify potential risk events. These considerations are listed in terms of:

- development projects and acquisition strategy;
- platform project; and
- the software component of a project.

While the considerations are listed separately in these sections, it is possible that a project will draw technical risk events from each of these categories.

The material below is drawn from 'Technical Risk Assessment: a Practitioner's Guide', J. O'Neill, N. Thakur and A. Duus, DSTO-GD-0493, 2007, with some small modifications.

A development project/acquisition strategy considerations

1. Is the proposed project approach technically sound? Will the technology work as specified in the required timeframe? Is the maturity of the technology a time and money issue, are there fundamental research breakthroughs required, or are there scaling or architectural issues?

2. What is the confidence that the project will run to completion? Does the contractor(s) have the resources and expertise to successfully deliver the contract?

3. If the project relies on a technology process (eg structural refurbishment), what confidence do we have that an Australian contractor (if involved) will be able to run the technology process to completion? What confidence do we have that the technology process will take the same amount of time when conducted by an Australian contractor on ADF platforms (with potentially different fatigue issues) compared with similar overseas processes? What is the impact on capability and schedule as a consequence of any uncertainty with the implementation of this technology process?

4. Are there any technical reasons why the proposed options will not meet Australian capability requirements?

5. What are the integration risks for the options working in the Australian environment?

6. Are there any certification issues involved in the options? Will Australia be accepting the 'first of type' and if so what issues need to be addressed? What is the trade-off between moving down the production line and allowing another country to bear many of the certification risks versus the delays into service from a capability perspective?

7. What regulatory hurdles need to be addressed before the capability system is successfully accepted into service (radio frequency emission licenses, environmental regulations, airworthiness certifications, etc)?

8. Have the 'right' technologies been locked in from a strategic perspective? By going down this particular technology path has the ADO locked itself out of a competing technology, or created longer-term support issues, such as increasing the cost of upgrades?

9. What are the implications for DSTO's science and technology support base? What risk treatment work does DSTO need to conduct up to acceptance into service testing? What through-life support will DSTO need to conduct for this project and what infrastructure and skill base will be required, for example, fatigue testing, development of tactics and doctrine, technology insertion for future upgrades?

10. Are there any consequences derived from the acquisition strategy? The contract will address the relationship between the prime contractor and individual sub-contractors. Responsibility for the development of different subsystems might lie with different sub-contractors, and integration of these into the system might be the responsibility of another. The Project S&T Adviser should be fully aware of these arrangements, and of the consequences for the assessment of technical risk. The proposed risk treatment strategies might also vary from one possible prime contractor to another.

11. What are the limitations with respect to the availability of technical information through export control and similar provisions, and what are the impacts on the technical risk assessments?

Platform project considerations

1. What are the potential issues in integrating the sub-systems onto the platform, including power, physical space, weight, heating, cooling, integration into existing data buses, information sharing, mission systems, electro-magnetic interference? Is there anything unique in this particular integration that might constitute a significant technical risk event?

2. What are the human systems aspects of the proposal? These aspects may include changes to data display screens, ability to process information, physical space issues in crew compartments, etc

3. What are the cumulative effects on the overall platform as a result of these integration issues (for example, is the platform now overweight, short on power, or at the limits of its processor's capacity)? Has the platform exceeded any design limitations, and if so, what is the impact?

4. Which sub-systems will need to be upgraded in what timeframes? Do the new sub-systems being integrated impact on the planned upgrade schedule (either positively or negatively)? Are there supportability issues emerging for any of the sub-systems?

5. How have the dependencies (cross system boundary flows) changed between this platform and the wider Defence environment as a result of this proposal?

Considerations of the software component of a project

1. What is the software architecture? How does this architecture integrate into the broader Defence Information Environment?

2. What are the capacity issues for this software in terms of the processor requirements, memory requirements, storage requirements, and network requirements? How do these capacity issues impact on other software projects? Will the current system software and application software support this new software or are upgrades required? If upgrades are required what other software projects are affected?

3. Will the current hardware environment support this software (hardware obsolescence management issues)? Hardware includes the computer system including all input and output devices.

4. What is the growth capacity for the software? Software systems are designed to handle a number of transactions per minute. What happens if the number of transactions doubles, triples or increases by an order of magnitude? Alternatively, how easy is it to add new functionality to the software and what is the impact? In both cases, the impact must be assessed not only in terms of the software architecture but the capacity issues listed above.

5. Are there any Intellectual Property issues or other issues that affect the release and supportability of the software including source code?

6. Is there sufficient technical expertise to develop the software, to support the software system for its life of type, and to maintain and update the software? A key point is that the technical expertise is different for each of these issues.