A Continuous Capability Development System

A (2021) white paper by Dr Alan Dyer
Ensuring delivery of capable systems in a dynamic world

14/07/2025

DyerNeed Pty Ltd

Contents

Introduction
Motivation
CCDS vision
CCDS components
Comparative measuring
Summary and key points
Annex A - Nuanced view of the capability levels
Annex B – CCDS components in additional detail

Mailing address: PO Box 162, Bungendore, NSW, 2621 - ABN 65 166 364 343 - Tel +61 4 1034 2771

Introduction

Document context

1. This document intends to describe a continuous capability development system (CCDS) that ensures an enduring capability; differing from the historical approach of ‘big bang’ projects. This document is presented within the context of large capability programs.

2. This paper was originally provided in draft form (in 2021) to Defence in the context of a large complex non-platform capability as a thought piece to provide a different perspective on delivery drivers and pathways. The development of this white paper was outside of any contracted work or deliverable, and the author is grateful to the Defence members who provided comment on the early drafts.

3. Since the original draft of this paper, Defence has adopted the concept of the continuous capability development and delivery (C2D2). This white paper is a polished form of the original draft; does not reflect the recent evolutions; and is published in recognition of the early conversations.

Key definitions

4. This paper aligns with a previously defined enterprise architecture framework (EAF). For ease of discussion; the following terms are used generically in this document in the following way:

   a. The **state** of ‘something’ is a series of measured characteristics. A more general (non-architectural) definition is ‘the condition of a person or thing, as with respect to circumstances or attributes’[1]

   b. An **effect** is the result, outcome, or consequence of an action. An effect can be described as a change in the state of a resource as a result of some activity.

   c. A **process** is formally defined in the BPMN standard as "A sequence or flow of Activities in an organization with the objective of carrying out work." The EAF considers a process to be synonymous to action, activity, task or workflow.

5. The concept of **work** is core to the description of states.

   a. In physics, entropy is a measure of disorder, and the Second Law of Thermodynamics states that all closed systems tend to maximize entropy.

   b. The level of disorder equates to a level of risk that desired effects or outcomes will not[2] be achieved.

   c. For the purposes of this paper, **work** is the expenditure of resources (including energy) to either maintain or increase the level of order – working against an increase in disorder.

6. **Maturity** describes a state of development. For the purposes of this document, an increase in maturity is directly related to a decrease in disorder. Maturity is often expressed as quantum levels based on metrics.

7. **Capability** is the power to achieve a desired operational effect in a nominated environment within a specified time and to sustain that effect for a designated period. Nominally, a capability improvement increases the power to achieve the desired effect, but in reality, a capability improvement more likely maintains the power to achieve a desired effect in a changing threat environment.

8. A **horizon**, within this paper, refers to how far in the future a person can ‘see’ with reasonable confidence and reflects a period for which a decision can be made at the start of the period with reasonable confidence that the original decision will still be valid at the end of the period. Any horizon mentioned in this

[1] Macquarie Dictionary, first definition

[2] Risk is adversity agnostic – the risk is really that outcomes will or will not be achieved.

paper is for illustrative purposes only; in the real world such horizons will be very context sensitive. Confidence, accuracy and precision are independent concepts.

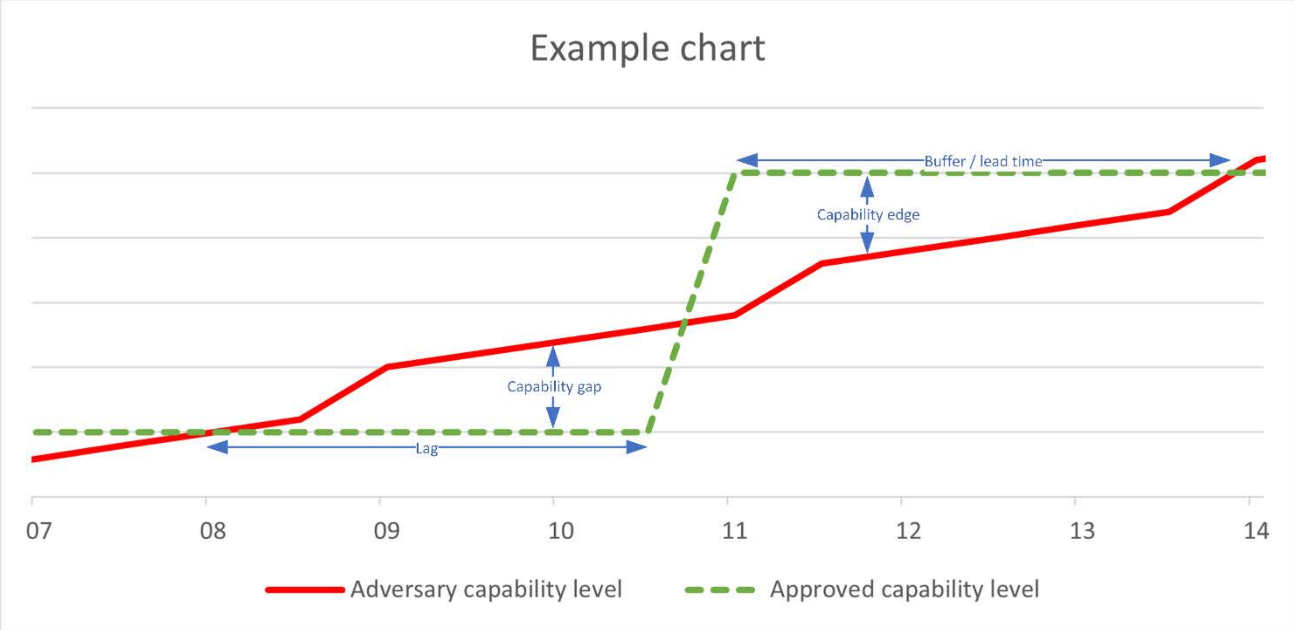

Figure 1: Capability comparison terms

9. In understanding how a delivered capability compares against a perceived or actual threat, the following terms are used. See Annex A for additional thinking on the comparative capabilities.

a. **Capability gap** – a deficit where the capability is unable to address the threat at a point in time.

b. **Capability edge** – a lead where the capability can address the threat at a point in time.

c. **Lag** – an indication of the time required for the capability to address the current threat.

d. **Buffer** or **lead time** – an indication of the time available before the threat level increases such that the capability edge becomes a capability gap.

e. The capability gap or edge are based on comparing the threat to the capability at a point in time.

f. The lag or buffer are based on comparing the parity between the threat and the capability across a time period.

10. Systems have different states: systems-in-being (S-IB), systems-in-acquisition (S-IA), systems-in-development (S-ID) and systems-under-design (S-UD). Any of these could be a system-under-test (S-UT).

Motivation

11. Traditionally, Defence (or the responsible agency) has delivered capability improvements in a accordance with a legacy capability development lifecycle. This lifecycle had been adjusted by the Kinnaird and Mortimer reviews, but were aligned with large platform projects. In a nutshell, the traditional project was based on well-defined[3] requirements up front with a lengthy approval and acquisition/delivery 'waterfall' process. Once the requirements were set, they were not changed without an additional approach to Government which could add years to the acquisition timeline. A typical project definition activity following the defined lifecycle would take at least seven years from conception to initial delivery.

[3] 'Well-defined' was subjective.

12. This lengthy waterfall approach meant that the functions and specifications for addressing future capability had to be addressed years in advance. The capability planners needed knowledge of the threat environment at least 7-10 years in advance. This is beyond most high-confidence assessment horizons (3-5 years).

13. Some projects planned for a mid-life technical refresh, but the budget for this refresh was set at the time of approval and could only assess the size of the refresh based on the extant assessments for the future threat.

14. To compound this lengthy legacy process, the effectiveness of the acquired systems was measured against the specifications that were set at the time of approval and often did not measure the capability impact against the contemporary threat. The underlying implicit[4] acquisition assumption is that the threat level against which the systems were pitted would not materially change during the life of the system.

15. Another factor in the legacy process was the assumption that each project was a stand-alone activity. Collaboration across projects was minimal and any understanding of cross-agency efficiencies was not used to effect – leading to re-work and duplication of effort. Industry was seen as a provider that must respond as Defence requires without any consideration of the state of the Industry at that time; or their ability to deliver over the life of the capability system.

16. Defence did have some processes for rapid acquisition, but these were limited by policy and regulation to one-shot operational acquisitions.

17. The main point is that, even with the best of intentions under the legacy approach, the capability systems cannot maintain the capability edge required to achieve the contemporary capability effect; even though the systems could be functioning well within the specifications originally agreed. Not only has an edge not been maintained, but is usually significantly lost, placing lives and systems at significant risk.

18. The First Principles Review of Defence reformed the capability lifecycle, which is continuing to mature[5]. While the general phases align to the legacy capability development lifecycle, the approval processes have been significantly overhauled. This also presented opportunities to review the delivery processes for capability systems.

19. The motivations for defining a CCDS include:

   a. Avoiding a capability gap

   b. Reducing the lag where a gap exists

   c. Avoiding long times between delivery of capability systems or upgrades which increases the lag when the capability edge becomes a gap.

20. The traditional 'big bang' approach to delivery increases risks of delays, changes in funding, risk in costing fidelity and increased risk of outdated requirements. Removing these risks is another motivation for the CCDS.

CCDS vision

21. The primary objective is to remain ahead of, or at least keep pace with, the threat. The Australian Government is also driving greater involvement of Australian sovereign industry.

22. A key vision associated with the objective is to reduce the necessary forecast horizon to reduce surprises and avoid system obsolescence caused by being overtaken by events or technology. The strategy to

[4] The people in the process often did understand that threats changed, but the process itself, based on a sequential waterfall process, did not allow for this reality.

[5] Late note: Defence, at the time of this belated publication, are now using the One Defence Capability System (ODCS)

achieve this vision will be to avoid the traditional 'big bang' delivery and adopt a more agile shorter-time frame delivery of smaller and sometimes riskier packages.

23. The use of smaller (and possibly riskier) packages allows Defence to place itself near the 'bleeding edge' when needed. This means that advanced systems are functional sooner and could already be in operation when a technology surprise emerges. The heavy involvement of research and development and short turn-around times for technology will mean that Defence can react in a timely manner to technology surprise.

24. To support the Australian Governments Industry strategies, a logical and managed approach that allows Australian Industry to evolve and deliver capability is needed.

25. The logical and managed approach for the CCDS should be based on recognised working practices, but perhaps employed in a novel setting. Some established practices to be considered are:

a. The Capability Life Cycle; treating the CCDS as a capability within itself and considering the fundamental inputs to capability (FIC).

b. Managing Successful Programs; activities within the CCDS will be analogous with those of a traditional program.

c. Capability Maturity Model; allowing for self-evaluation of the CCDS to fine tune performance as well as providing insights into the ability of the EW capability to address the contemporary threats.

26. The US have a continuous capability development and delivery program (C2D2) relating to the Joint Strike Fighter; but publicly available documents note that this is a software development initiative and not related to the platform as a whole. The CCDS described in this paper aims for a broader impact in a more complex capability and operational environment.

27. Annex A places the lags and gaps in the context of various approval horizons, and illustrates a quantitative perspective.

CCDS components

28. The simple vision statement "remain ahead of the threat" reveals key drivers for components:

a. "threat" implies an understanding of the threat at any point in time. This drives the need for awareness.

b. "ahead" implies an understanding of the comparative nature between the capability and the threat – including the application of emerging technologies on either side of the equation. This drives a need for measurement and evaluation.

c. "remain" implies a non-static environment and subtly implies a system moving forwards (not backwards). This drives a need for ongoing activity instead of a single time-bounded activity.

29. Borrowing concepts from Managing Successful Programs reveals six main considerations:

a. represent the capability to external stakeholders

b. manage whole of capability strategy, roadmap and design

c. manage the Products

d. prioritise and coordinate change activities

e. enable continuous evolution and innovation

f. manage funding and other resources.

30. Of the six considerations listed above, three are normally addressed by the combined team that manages the capability. The other three are usually addressed by sub-teams with that specific focus:

a. A capability definition team that manages the whole of capability strategy, roadmap and design.

b. Product management teams that manage the Products, including configuration, baselines and technical design of products-in-being.

c. Various project management teams that manage the change activities, although the change activities are likely to be prioritised and coordinated by the capability definition team (in line with higher authority approvals)

31. Within the capability development environment, the scope of change management is vexed. At one level (capital delivery), change management is performed through projects (or programs) following established frameworks. At the other level (sustainment delivery), change management is performed through engineering frameworks and is more likely managed by the Product teams rather than project teams. This line can sometimes be very grey.

32. A simple systems paradigm considers people, process, technology and the environment (natural and built)[6]. While people (the team), process (the listed activities) and technology (Products) are covered by the considerations listed above, the environment is the additional dimension that is often given only minor consideration during the design of systems.

33. In summary, the design of the CCDS must include functions that address the:

a. Environment

b. Capability definition (strategy, roadmap and design)

c. Products

d. Change activities

e. Evolution and innovation

f. Funding and resources

34. The CCDS must also engage with external stakeholders, but this is embedded within the functions listed.

35. The CCDS will initiate or enable the following activities but is unlikely to directly control:

a. Change activities (capital acquisition). The CCDS will facilitate approval, funding and resources for capital acquisition but the assigned project team will conduct the change. The CCDS will remain a stakeholder for the purposes of confirming the needs.

b. Specific R&D projects. The CCDS will facilitate approval, funding and resources for some R&D projects, but will only be a stakeholder for the purposes of the R&D output. This will not apply to all R&D projects, some will be firmly within the remit of the CCDS.

c. Capability effects. The CCDS creates the environment of the delivery of capability systems (including the necessary fundamental inputs to capability), but the customers of the CCDS operate the capability systems to achieve the desired capability effect.

[6] Originally systems engineering approaches only identify the people, processes and technology. Slade Beard included the environment as an important driver for system performance and identified that this environment could be ‘natural’ (as existing independent of the presence of the system) or 'built' (as in designed and acquired as part of the system).

d. Products. The CCDS sets up the product management framework to ensure that what has been delivered continues to work as intended. The Product Management teams will undertake the management based on guidance from the CCDS.

e. CMDV&V. The activities required to verify and validate capability systems and capability processes will be driven by the CCDS. The performance of the verification and validation will be the responsibility of specialist units that will work across multiple programs. This work will also include, or link to, the tactics validation and relevant modelling and simulation.

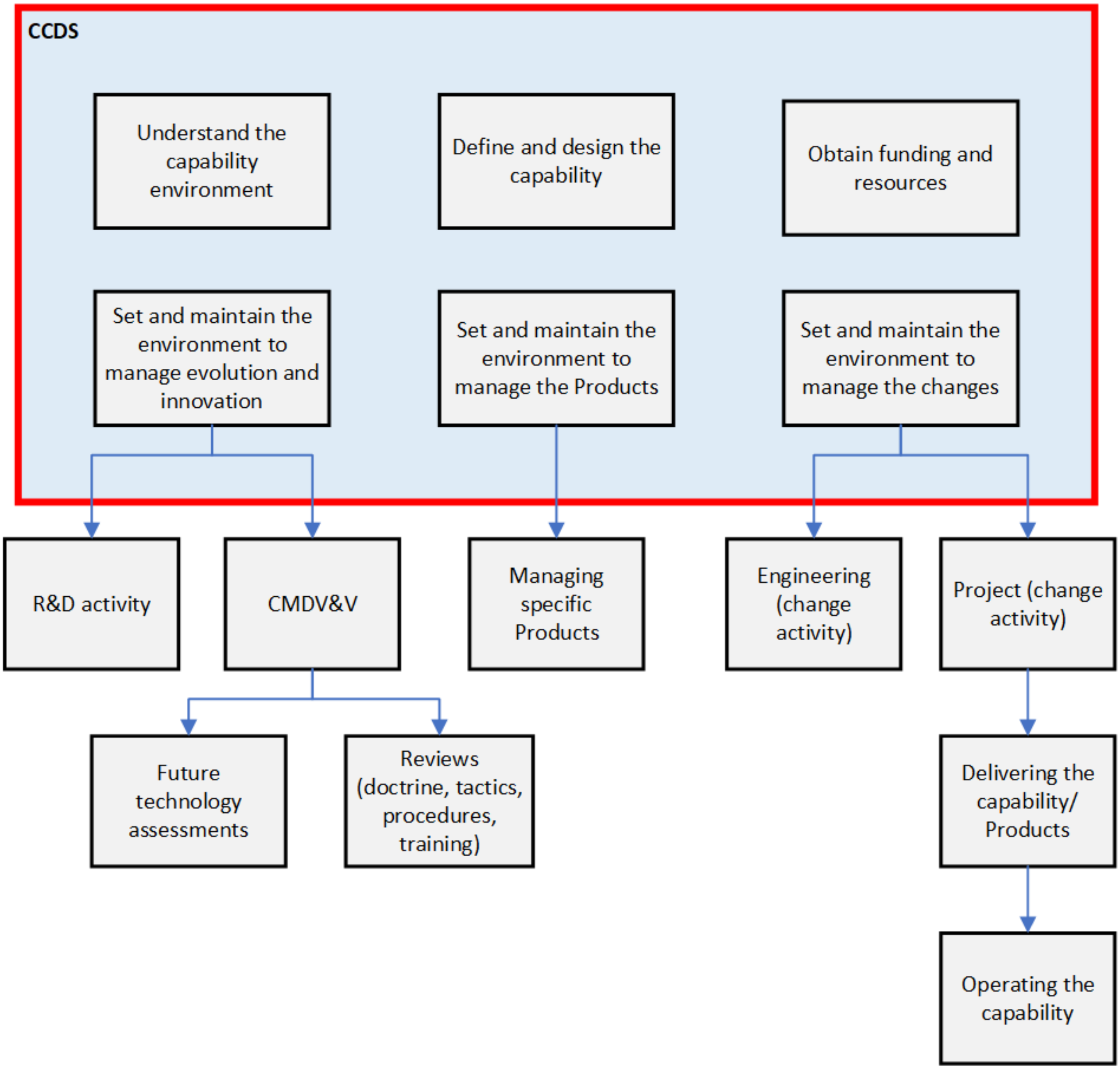

Figure 2: Scope

36. Each component of the CCDS will achieve the outcome through defined processes, which can only be effective with the right people and resources. In some cases, dedicated facilities or a specialised workforce will be critical.

Comparative measuring

37. Comparative measuring should use agreed metrics to determine the state of the capability at any point in time. Typical events where the state is assessed are at the determination of initial operating capability (IOC) and post-modification evaluation.

38. In some cases, these metrics will be used against defined performance targets (indicators) to determine if the capability has reached particular states. This work will align with the test and evaluation categories, and will determine if the capability meets the minimum, desired or operational levels of capability (MLOC, DLOC and OLOC). MLOC could also be considered as the IOC.

39. The comparative measuring system must be valid and consistent over time and cannot be based on absolute measures that are tied to particular systems (threat and own) at a particular point in time. The comparative measuring system must also be valid for both synthetic and real-world environments testing. However, the comparative measuring system must be able to use contemporary absolute measures in the comparative framework.

40. Ideally the comparative measures will be linked to the capability effect and will be used to determine if the capability systems can achieve the agreed outcomes in context.

41. Depending on the functions and effects involved, some measures will be objective, and others subjective. The standards against which the measures should be applied will relate to the capability effects and agreed levels. Examples of such levels include:

a. Inferior. The measured characteristics indicate that the capability cannot meet the desired level of capability. The threat dominates in the measured environment.

b. Parity. The measured characteristics indicate that the capability can match the threat but does not dominate.

c. Superiority. The measured characteristics indicate that the capability will often achieve the desired effect in the measured environment, but not all the time.

d. Supremacy. The measured characteristics indicate that the capability will dominate over the threat in the measured environment.

42. Trying to achieve supremacy all the time is unrealistic. Reaching parity could be a threshold for an initial capability and reaching superiority in defined scenarios could be desired. These levels must be more clearly defined in context.

43. Another approach to understanding comparative measuring is the use of critical operational issues (COI), as defined in the Defence systems engineering environment. The formal definition from the Defence Glossary is that a COI is “an issue deemed critical because, if not resolved, could lead to the failure of a materiel system to achieve Operational Release”. This formal definition is limited in that it only addresses the delivery of systems as part of acquisition and does not address the ongoing evaluation of the capability system to achieve the capability effect. COIs are normally expressed as a high-level question that the Capability System must address and should be solution-class independent. COI are typically binary questions – ‘yes’ or ‘no’.

Summary and key points

44. The CCDS is a concept that recognises the limitations of traditional platform-centric acquisition approaches in a dynamic threat environment. It provides a structured means to ensure a capability remains effective over multiple Product lifetimes; replacing a legacy approach based on discrete projects with an early requirements-definition approach.

45. The CCDS addresses understanding the capability environment, capability definition and design, Product and change management, evolution and innovation, and funding and resourcing. As described here is consistent with a defined architecture framework, and aligns with the FIC for use in both the architecture framework and the capability lifecycle.

Annex A - Nuanced view of the capability levels

Introduction

46. The main body of this document introduces the concept of comparing a threat level against a capability level. The definition and measuring of any particular levels is outside the scope of this document. This annex provides additional detail, albeit still at a conceptual level, to illustrate the enormity of lagging capability levels within traditional acquisition pathways.

47. In these examples, the requirements are initially set ('approved') at year 0.

A simplified legacy perspective on edges and gaps

48. In the following two figures, the threat capability improves incrementally, but the three acquisition timelines are based on early requirements definition in a waterfall process. Included is a mid-life refresh. For the purposes of the figure, the time between the confirmation of requirements (year 0) and the initial delivery of capability (year 2) has been compressed from what might have been experienced under legacy Defence acquisition paths – a more exemplary timeframe would have resulted in possibly never addressing the gap.

a. The first figure emphasises how the capability level steps up over time.

b. The second figure emphasises the edge/gap over the time period. The aim of capability evolution is to stay above the threat line.

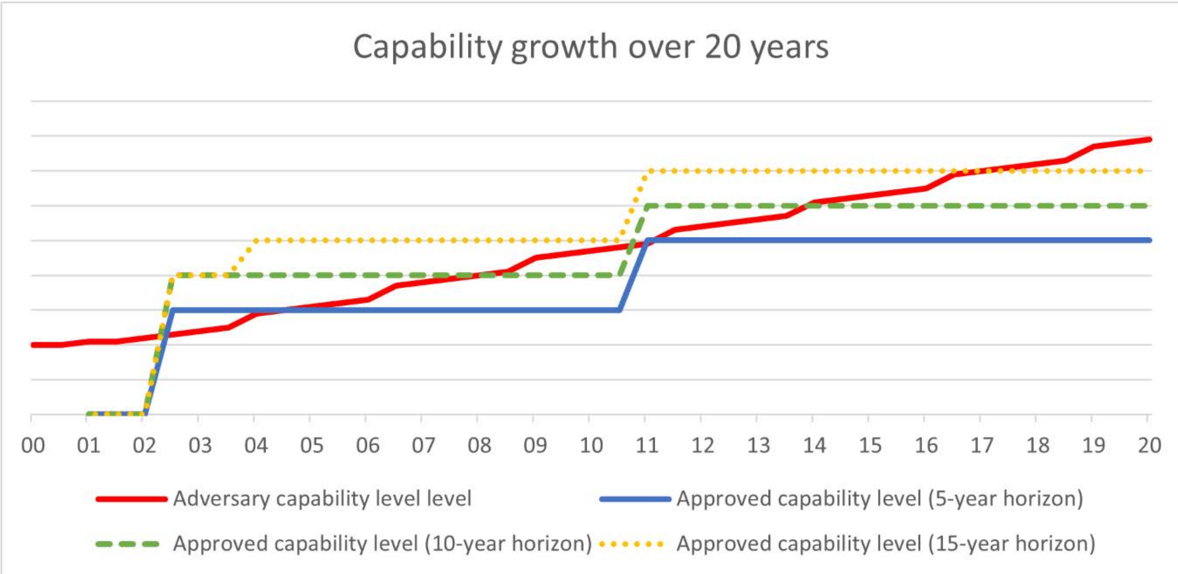

Figure 3: Capability levels based on generic growth (simplified legacy example)

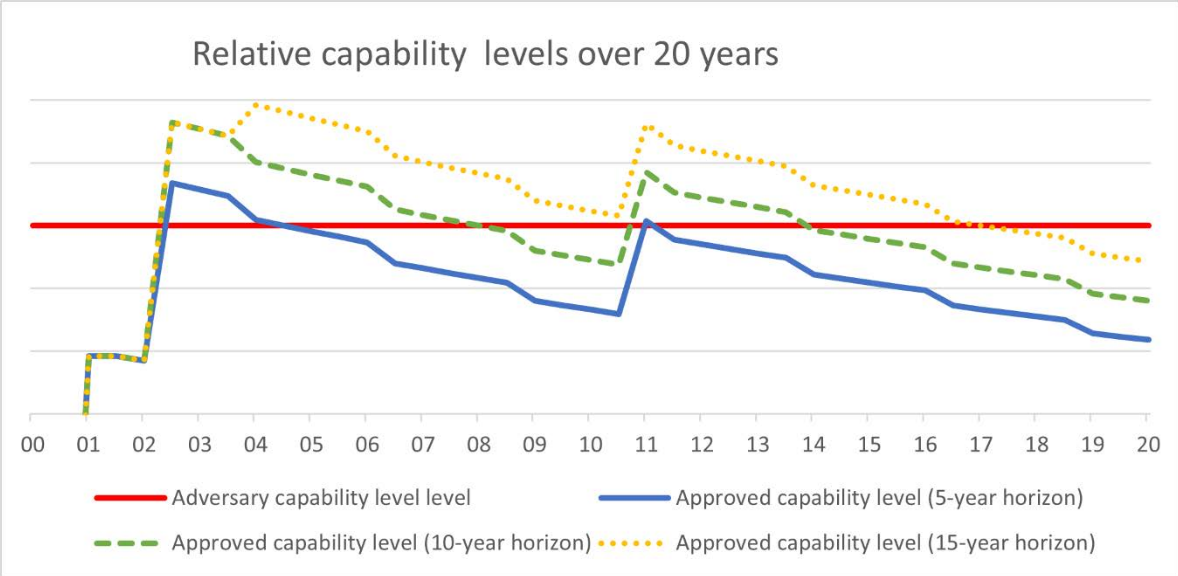

Figure 4: Capability levels relative to the contemporary threat (simplified legacy example)

49. The horizons in the two figures refer to an assessment horizon; with a commensurate initial capability increase – however an assessment horizon greater than 5 years is extremely unlikely. The threat level assumes incremental growth and does not include any technology surprises during the 20-year span. The mid-life refresh occurs at year 11; the acquisition based on a 15-year assessment horizon has an additional delivery step to address a possible capacity limit in Industry.

50. The main point to be taken away from the above figures is that even with the best of intentions under the legacy approach, the capability systems cannot maintain the capability edge required to achieve the contemporary capability effect; even though the systems could be functioning well within the specifications originally agreed. Not only has an edge not been maintained, but has been significantly lost, placing lives and systems at significant risk.

A CCDS perspective on edges and gaps

51. The following figures illustrate how the capability can maintain parity or superiority with the threat within a CCDS context. These figures are based on the same threat growth in the previous section. As per the previous section, the first figure emphasises how the capability level steps up over time and the second figure emphasises the edge/gap over the time period.

52. Rather than a 20-year acquisition path with a mid-life refresh, this CCDS example uses a five-year cycle where planning for the next tranche occurs in parallel with the in-flight acquisition. This means that the assessment horizon can be minimised without the long-term detriment seen under legacy constraints.

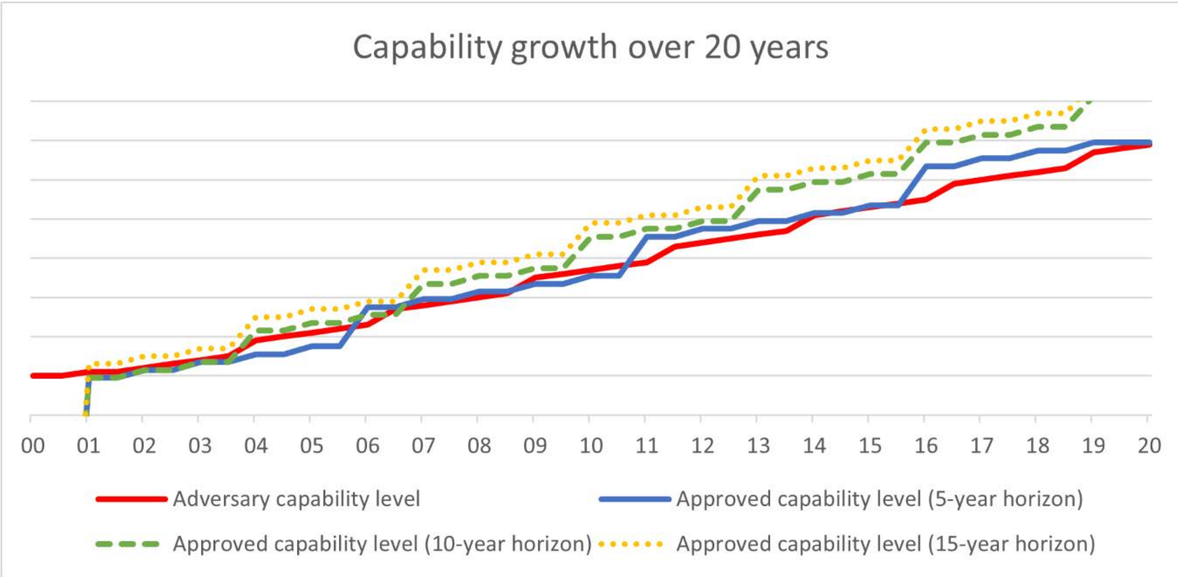

Figure 5: Capability levels based on generic growth (simplified CCDS example)

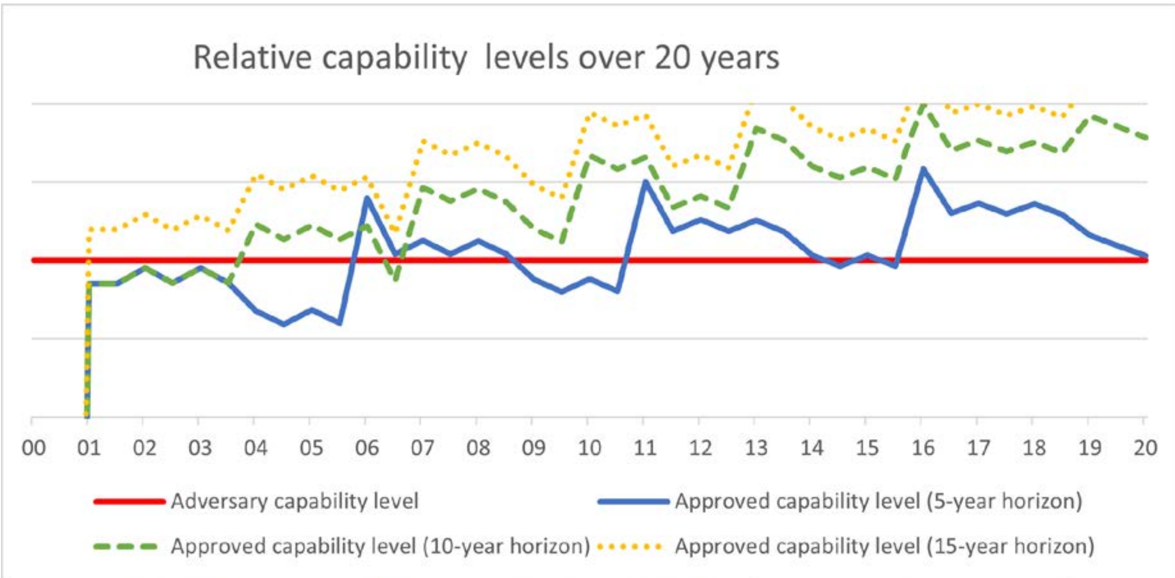

Figure 6: Capability levels relative to the contemporary threat (simplified CCDS example)

53. While the example here uses a five-year cycle, a three-year cycle with a five-year horizon would probably remain at parity or ahead of the threat throughout the life of the capability. In other words, a three-year cycle based on current knowledge and assessments of emerging technology will provide a better buffer against the increasing threat.

Innovative surprise

54. The previous sections assumed a relatively stable growth in the adversary capability level. Adversaries are non-cooperative and may develop disruptive technology or procedures that gives them some significant capability advantage. The discussion and figures in this section assume a threat 'surprise' 12 years into the capability growth.

55. The first figure illustrates the legacy approach with the mid-life technology refresh as already shown in the main body.

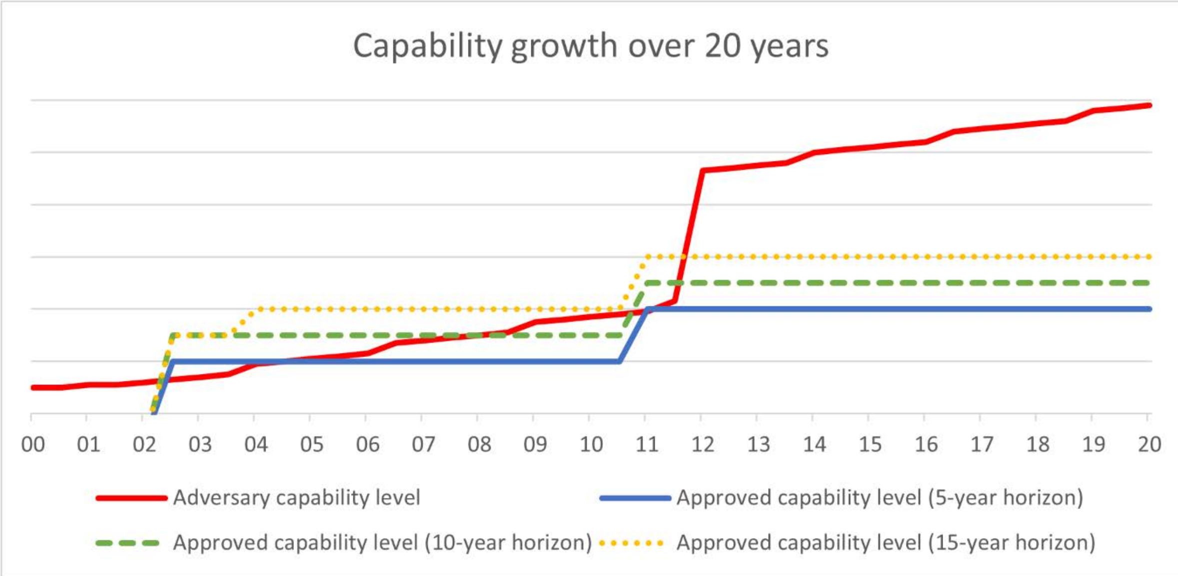

Figure 7: The impact of surprise on the capability edge (legacy)

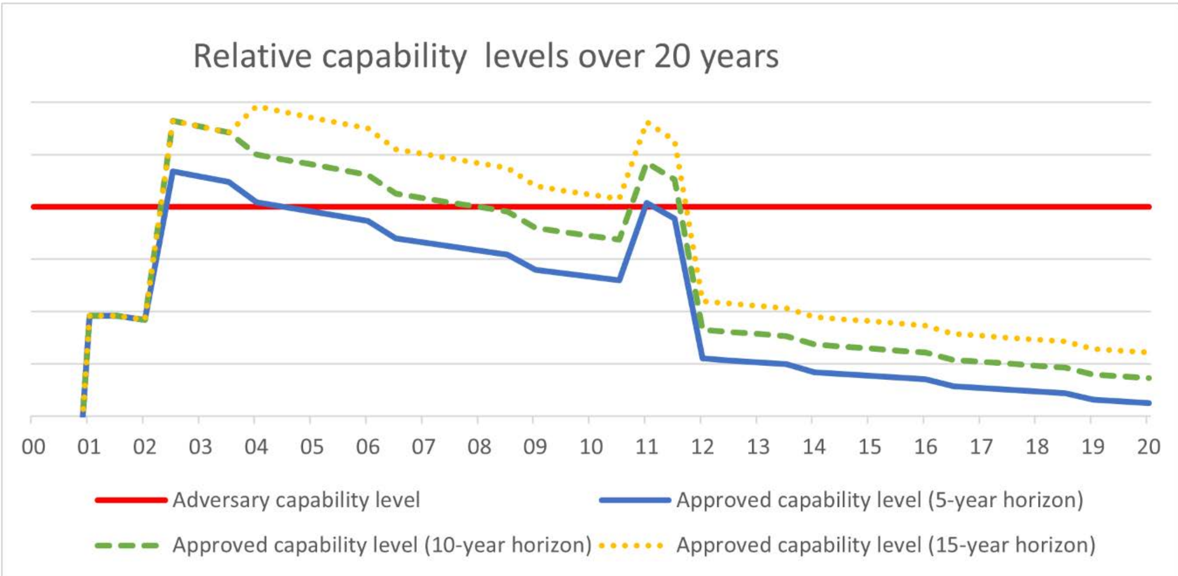

Figure 8: The impact of surprise on the relative capability edge (legacy)

56. The impact of this surprise is to wipe out any capability edge and introduces a lag of many years as a new project is stood up address the growth in threat. Under the traditional approach based on the Kinnaird and Mortimer reviews, at least seven years would be required to field new systems.

57. The proposed CCDS shows more resilience against this kind of surprise.

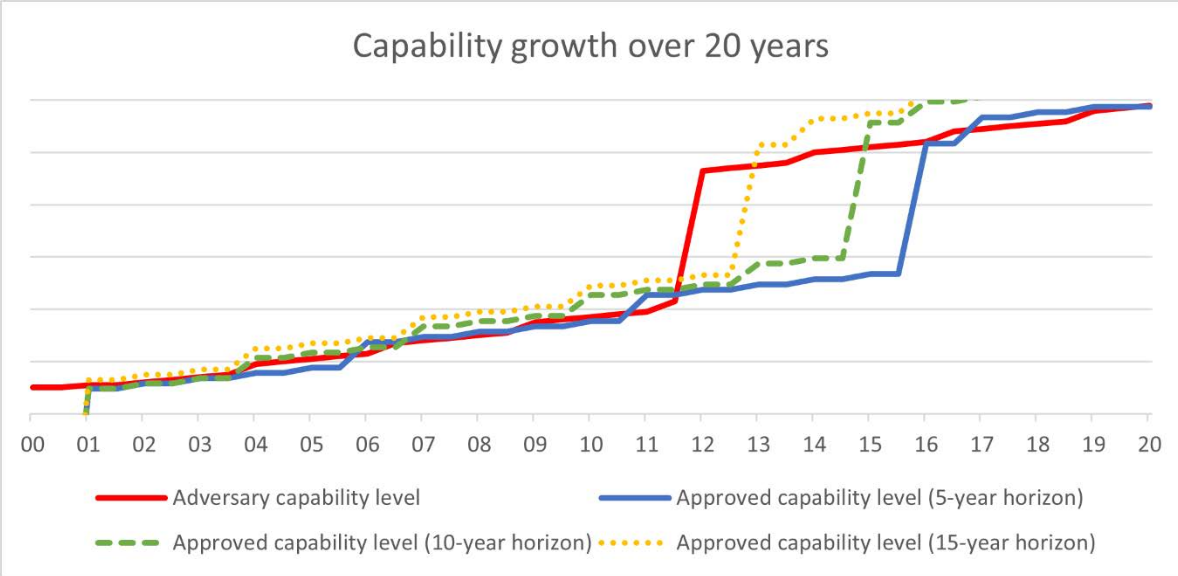

Figure 9: The impact of surprise on the capability edge (CCDS)

58. The five-year cycle of assessment could introduce a lag of up to 5 years, which is still an improvement over the traditional approach. A more rapid assessment cycle reduces this lag, although the full-cycle capability delivery processes may have an impact. Effective forecasting reduces the chances that such a capability leap is a 'surprise' and allows planning to occur before the new threat is fielded. This will allow a rapid response to the rising threat and provide opportunities to ensure a continuing capability edge. The relative figure helps illustrate this.

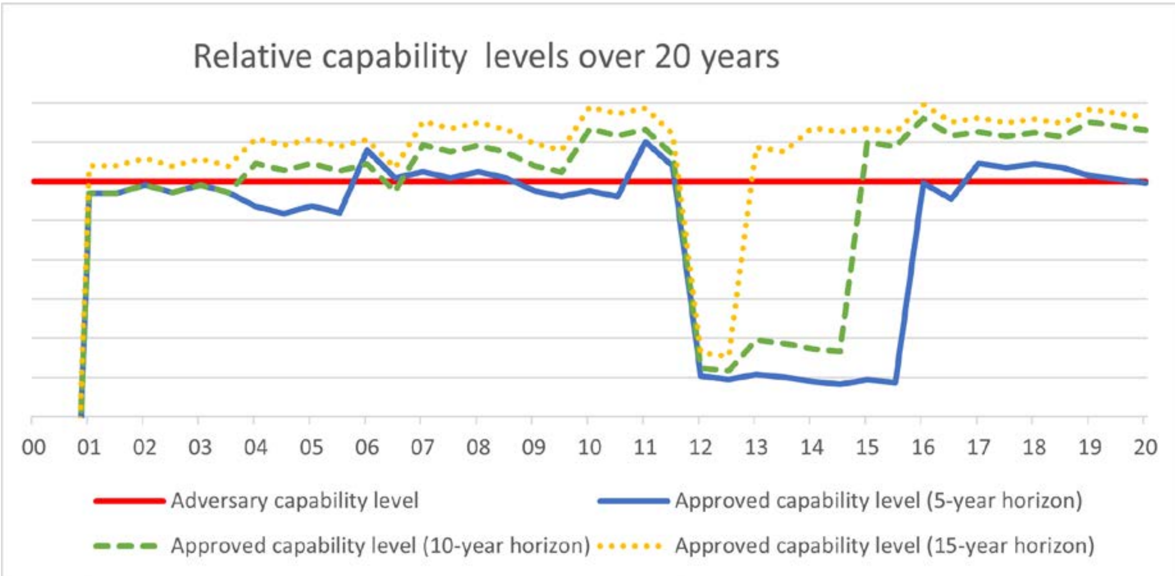

Figure 10: The impact of surprise on the relative capability edge (CCDS)

59. The corollary of this latter discussion is that the CCDS may open up additional innovation and allow Defence's own capability to deliver the 'surprise', producing an unexpected but welcome capability edge well in advance of the adversary. In this circumstance, the adversary will be trying to catch up.

Assessment uncertainty

60. The previous sections assume a degree of precision and accuracy in the adversary capability forecasts, which is not reflective of a real world. For the purposes of this part of discussion, only one line of capability

growth is shown for clarity and a near-linear growth in uncertainty is assumed even though a geometric growth in uncertainty is more likely.

The legacy view

61. The simple legacy approach is shown in the following figure.

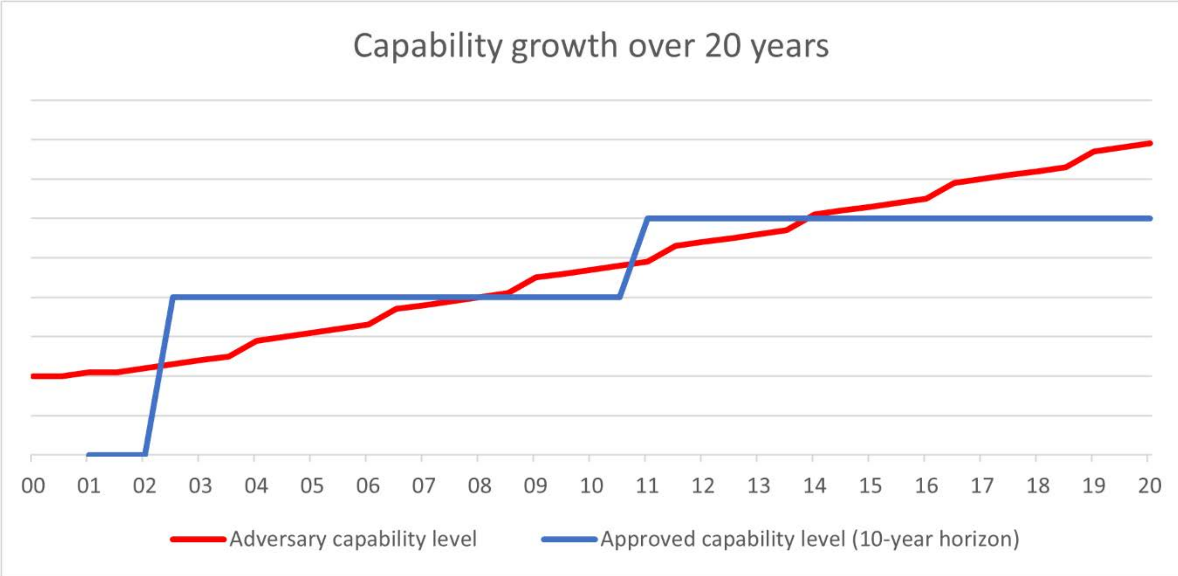

Figure 11: Assessed threat against planned capability (legacy)

62. The figure shows that a capability edge exists during years 2-8 and years 11-14. However, this assumes that the assessment of the threat level is accurate. The level of uncertainty about an assessment increases with the age of the assessment, or the forecast horizon used for the assessment. Correspondingly, our own capability levels are likely to be maintained within a level of tolerance.

63. The following figure shows the impact of uncertainty through the error bars.

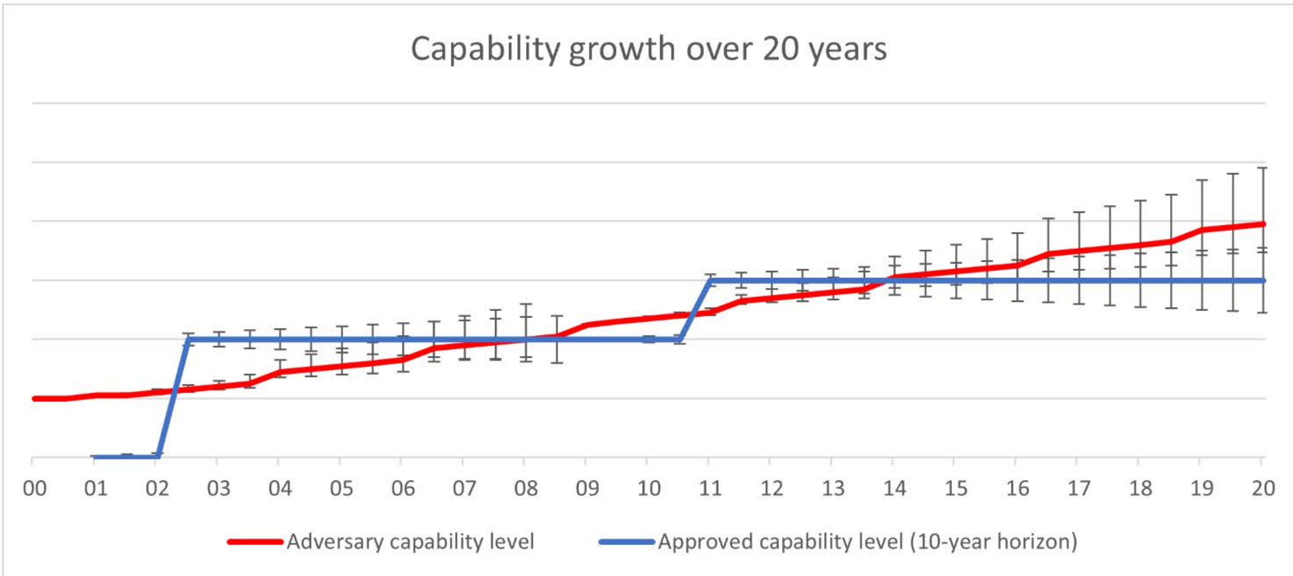

Figure 12: Assessed threat with a degree of uncertainty against planned capability (legacy)

64. The figure shows that the potential upper bound of the threat increases with time. Potentially, the capability edge now may only be available during the years 2-4 and year 11. The following figure clarifies the

capabilities if a 'bad case' perspective (where the adversary capability improves better than forecast, and the capability level declines due to limits in sustainment) is considered.

Figure 13: The extremes of uncertainty comparison of capability (legacy)

The simple CCDS view

65. The uncertainty in forecasting or maintaining capability is also a consideration when viewing the CCDS approach. As shown in the following figure, an increasing capability edge is available with the simple figures.

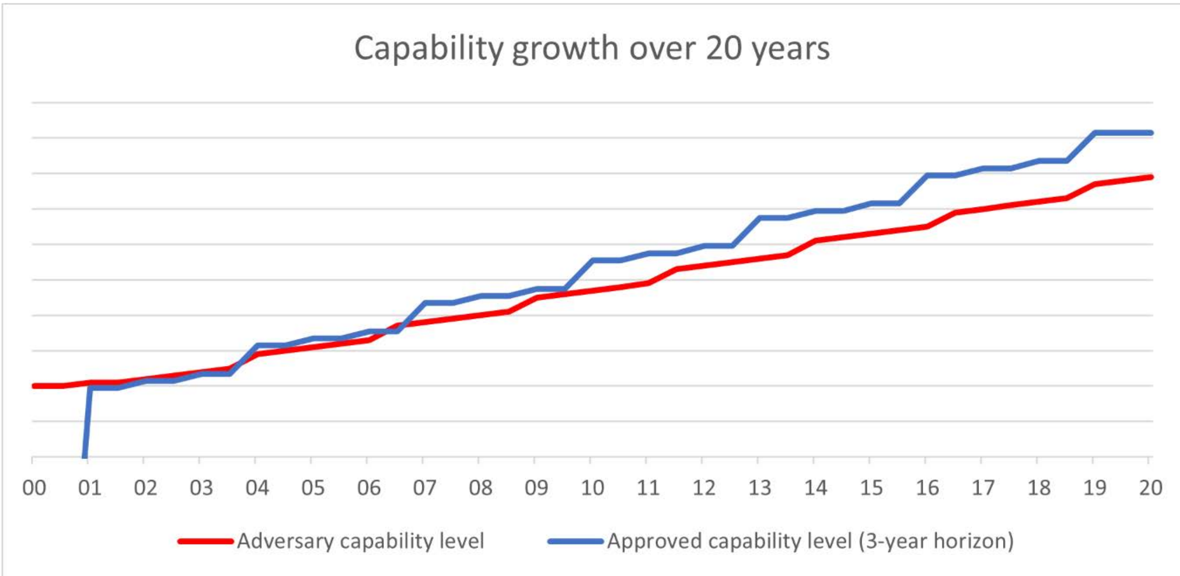

Figure 14: Assessed threat against planned capability (CCDS)

66. However, the edge could disappear when the assessment uncertainty is included. Because of the near-continuous nature of development and assessment, the impact of uncertainty is decreased.

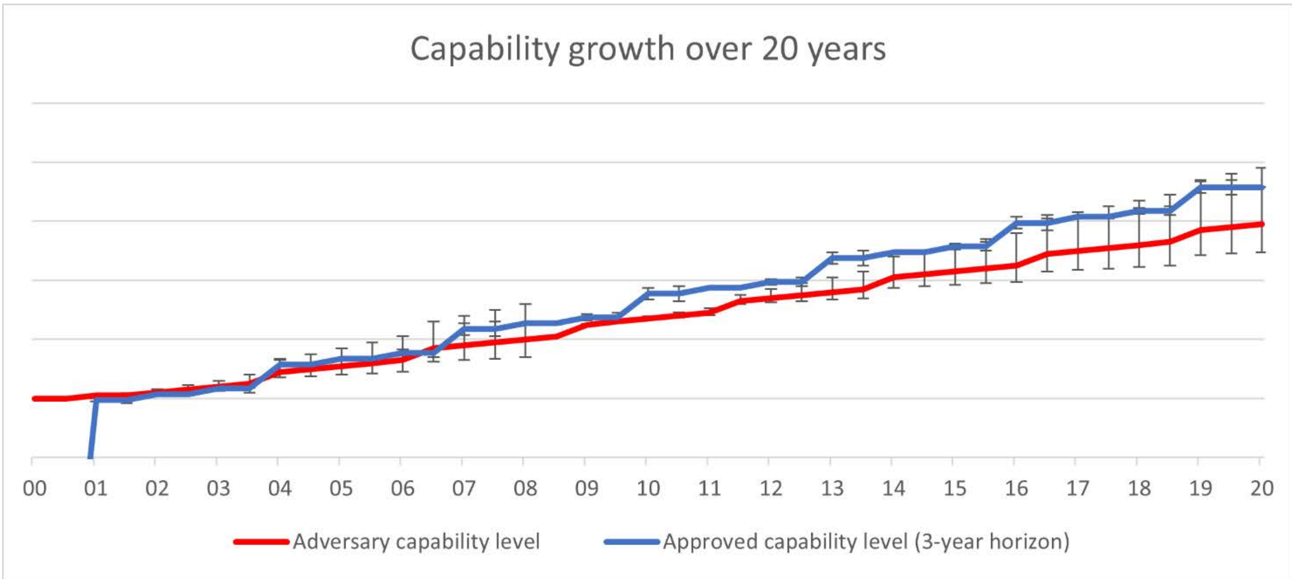

Figure 15: Assessed threat with a degree of uncertainty against planned capability (CCDS)

67. The next figure illustrates the bad case scenario with similar parameters to the figure used in the legacy section.

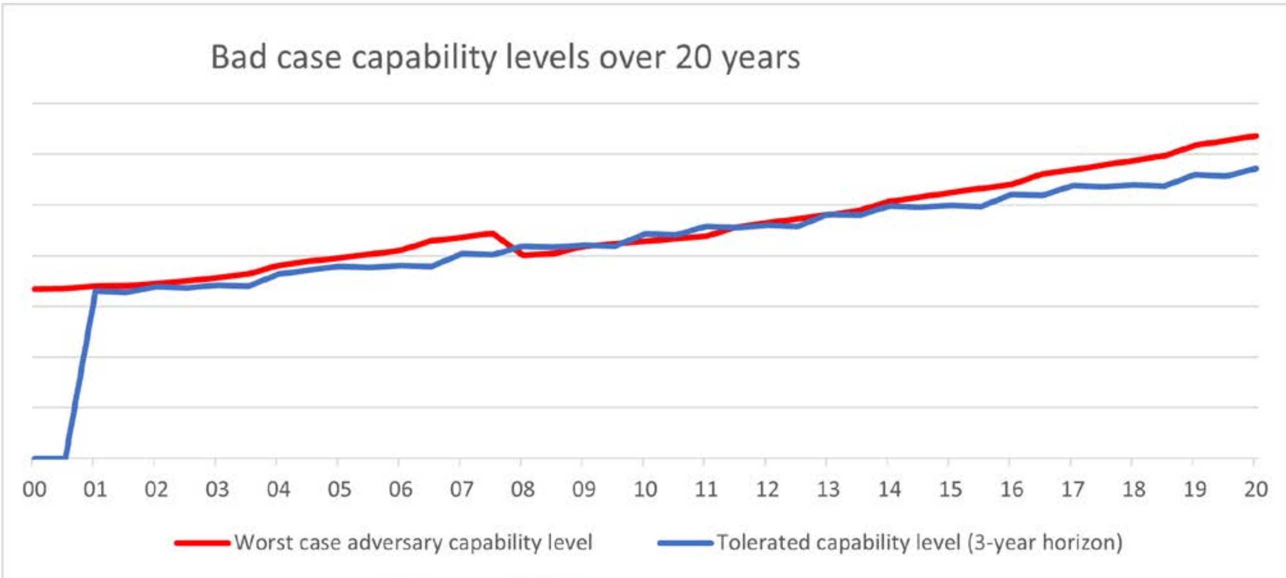

Figure 16: The extremes of uncertainty comparison of capability (CCDS)

A more advanced CCDS view

68. The above figures show a simple three-year cycle of assessment and capability growth. A pro-active assessment with additional forecasting support (e.g. through targeted modelling and simulation), as already included in figures in the main body, provide an additional buffer against uncertainty, as shown in the next two figures.

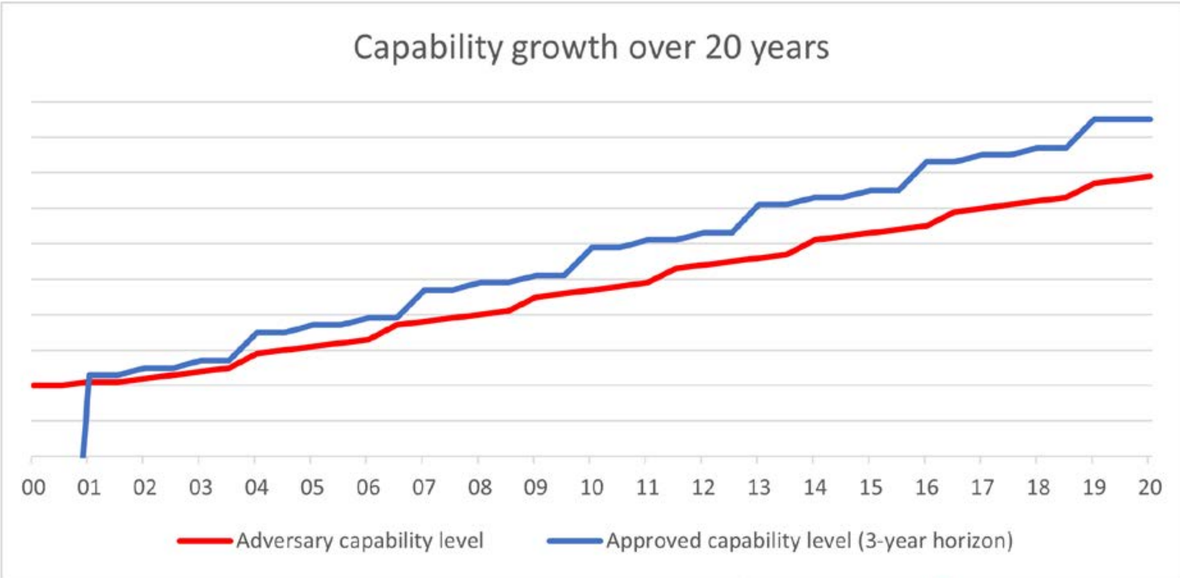

Figure 17: Assessed threat against planned capability (CCDS with forecasting)

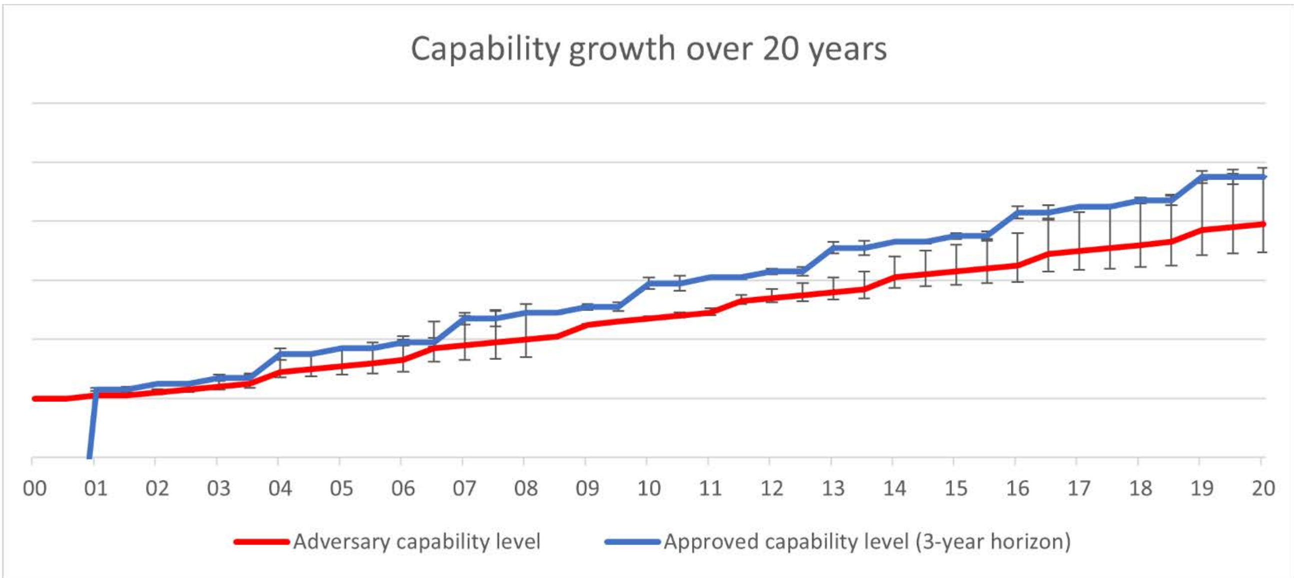

Figure 18: Assessed threat with a degree of uncertainty against planned capability (CCDS with forecasting)

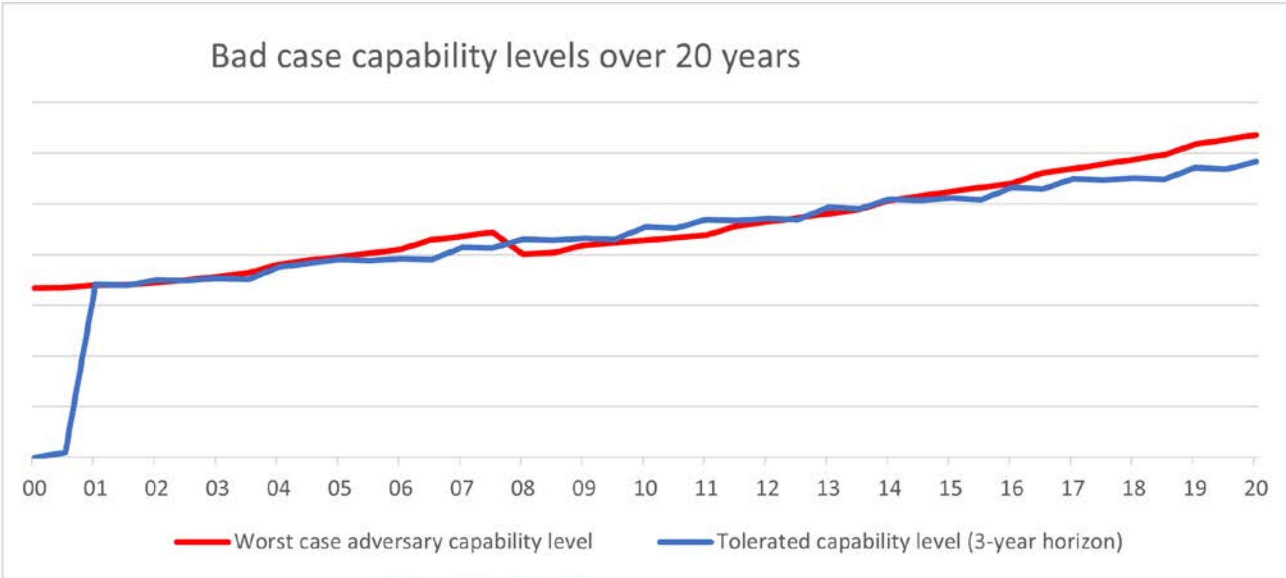

Figure 19: The extremes of uncertainty comparison of capability (CCDS with forecasting)

Relatively speaking

69. The bad case examples above show that our own capability is struggling to maintain parity with the adversary, noting that they are simple examples without surprises on any side. In these bad cases, the CCDS approaches minimise the gaps and the capability managers would be adjusting their capability tolerances to address that gap – the real world is the not the simple 'set and forget' that these simple examples can imply.

70. The following figure illustrates the comparative gap between the legacy, simple CCDS and CCDS with forecasting approaches in the bad case scenario.

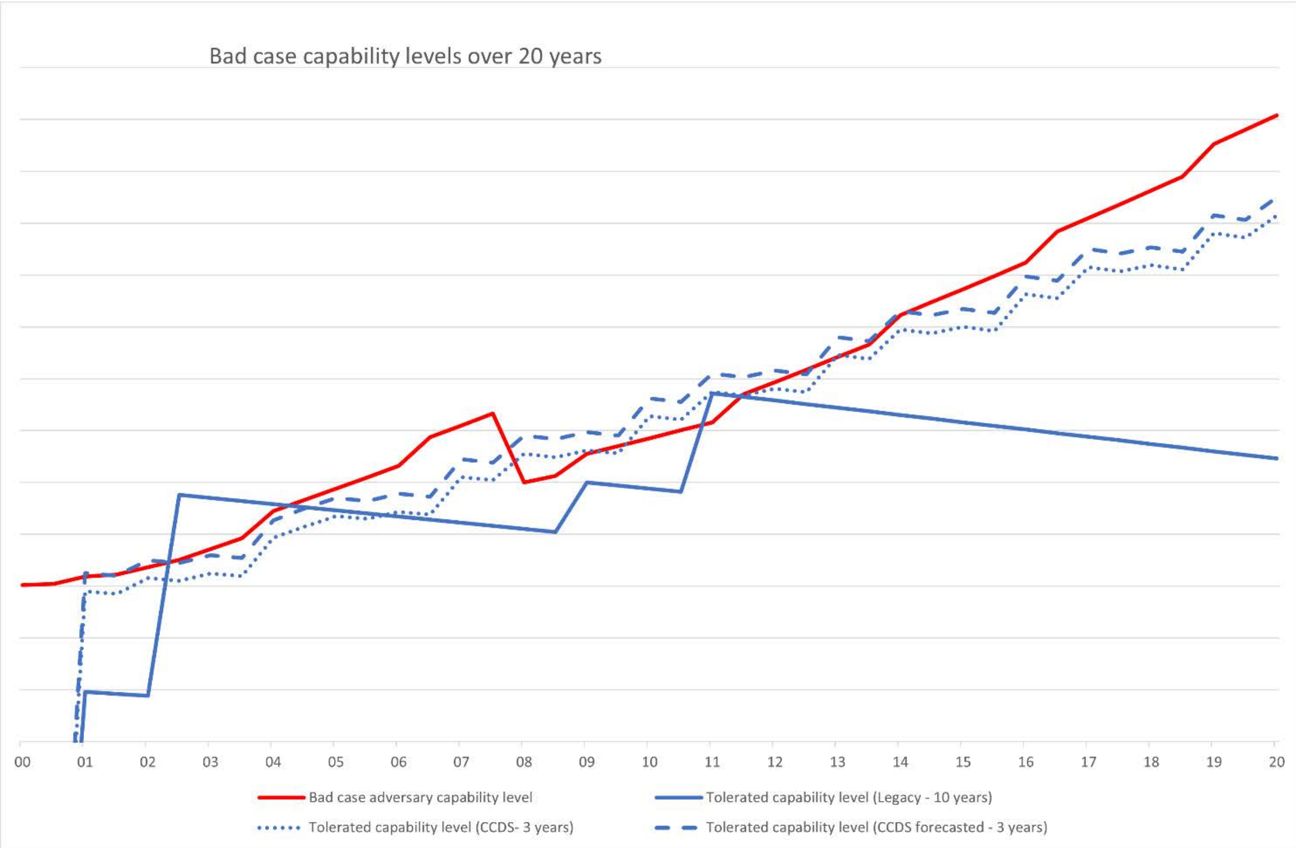

Figure 20: comparison between the various approaches in the bad case scenario

Annex B – CCDS components in additional detail

Introduction

71. The main section introduced the concept of components that would be useful in realising the CCDS benefits. This Annex addresses those components in a little more detail, noting that the definition of the components will depend on the capability under examination.

Understanding the environment

72. The key outcome from this component is knowledge of the comparative capability against the defined metric to address the threat – the capability gap or capability edge.

73. At its simplest, the ability to understand the capability gap or capability edge relies on:

a. Understanding the threat environment

b. Understanding the ability of the capability systems under consideration

c. Comparing both of these in the operational/mission context

74. Context is important. The threat environment is not a homogenous environment and understanding the gap is not necessarily achieved by measuring 'like for like'.

75. The elements involved in understanding the threat environment are:

a. Assessments (including intelligence assessments) of the threat. The level of certainty for the assessment will usually decrease the further out the assessment looks.

b. Simulations of the threat environment in different contexts, covering a range of environment conditions.

76. The elements involved in understanding the capability systems include:

a. Operational evaluation for S-IB

b. Post-activity reports for S-IB used in active environments

c. Exercise environments for S-IB or S-IA to create a range of stressed environments simulating potential scenarios

d. Hardware-in-the-loop and software-in-the-loop testing of systems (S-IB, S-IA, S-ID)

e. Function and performance specifications for S-UD.

77. The following figure illustrates the resources required to achieve the CCDS environment component outcomes.

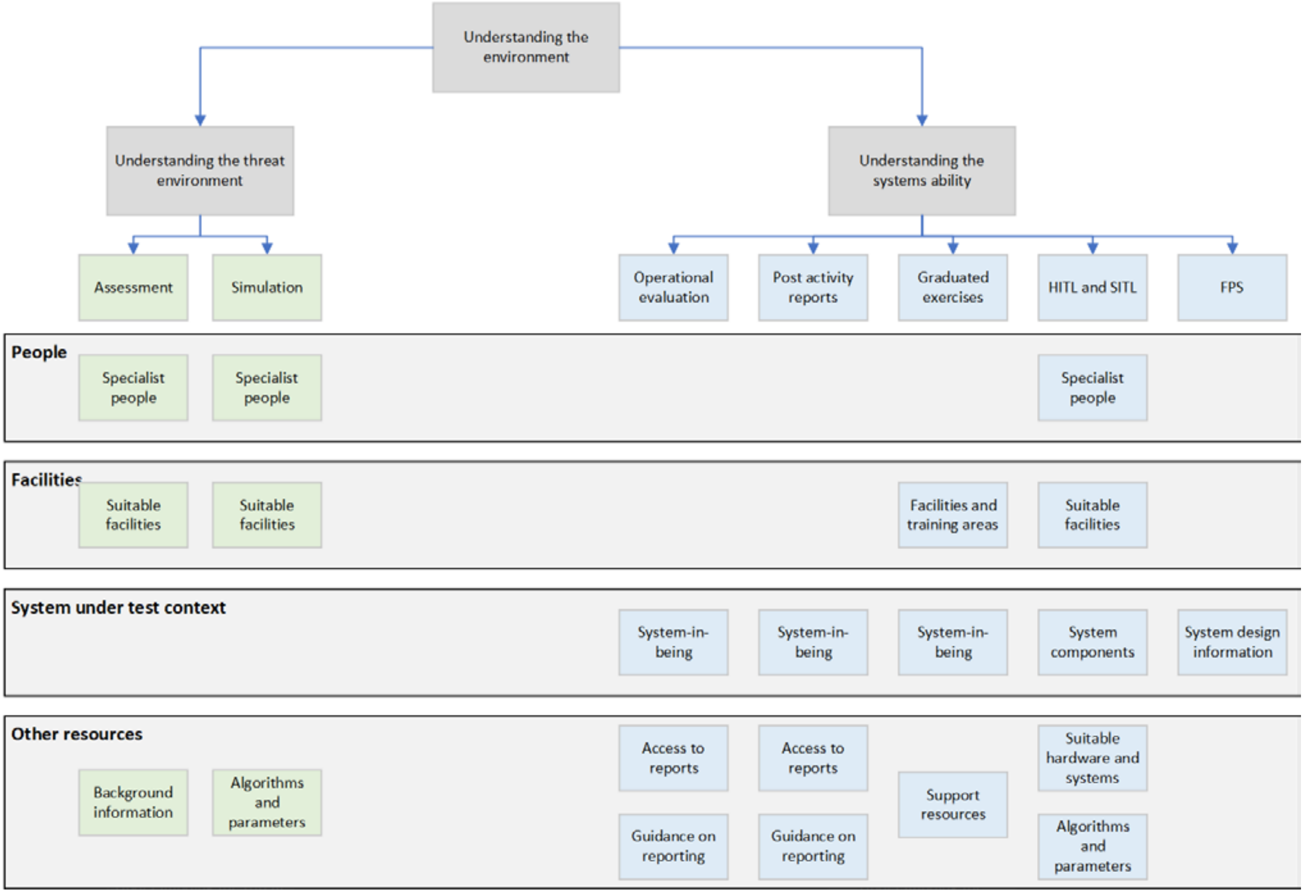

Figure 21: Considerations for the 'understanding environment' component

Capability definition

78. The key outcome from this component is an agreed capability design, consisting of a strategy and roadmap, and system or element designs. The capability design can be considered a Product; placing it under Product and Change Management control.

79. As a support system, the CCDS will also feature in the capability design as a Product; placing it under Product and Change Management control.

80. The elements involved in creating and maintaining the agreed capability design are:

a. Assessments of whether the design is fit for purpose, in that it accurately portrays the intent and effectively communicates that intent to the relevant stakeholders

b. Assessments of changes to guidance and how these may require changes to the capability design

c. Assessments of information relating to the evaluation of capability systems and how these may require changes to the capability design (changes to the systems-in-being are part of Product Management)

d. Assessments of the ‘hot tips and good ideas’ and how these can add value to the intent or Defence Outcomes

e. Designers[7] to create or update the appropriate part of the design

[7] The term “designers” is used here in a generic sense and could include architects, designers or engineers.

f. A governance framework to get agreement of the design from the relevant stakeholders.

81. In the Defence context, the external stakeholders that will agree[8] on the design should be:

a. Force Design and the relevant Capability Manager for the strategy and high-level roadmap

b. Capability Manager for the middle-level roadmaps

c. Engineering authorities for technical designs

82. Inherent in this activity is the ability to communicate the design to those who need it. Examples of external stakeholders and their use include:

a. The Government for funding approval; through the various committees and forums for endorsement and interim approvals

b. Industry, and in particular Australian Industry, for strategic Business and Industry Capability Development

c. Delivery agencies and project teams for capability delivery

d. Capability Managers for capability realisation across the fundamental inputs to capability

e. Product Managers for guidance on whether their Products remain fit-for-purpose

f. Product Managers for guidance on the sustenance, maintenance and disposal of their Products

g. Engineers for guidance on risks and issues relating to capability systems

h. Capability Managers for insight on how strategic and operational gaps will be addressed; this is separate from their role in funding approval but is part of their role in providing guidance

i. Tactics and operational policy developers for insight on how the capability systems can be used to achieve the capability effect in a joint environment

83. The following figure illustrates the resources required to achieve the CCDS capability definition component outcomes.

[8] 'Agree', 'approve' or 'endorse' may be verbs used in this context.

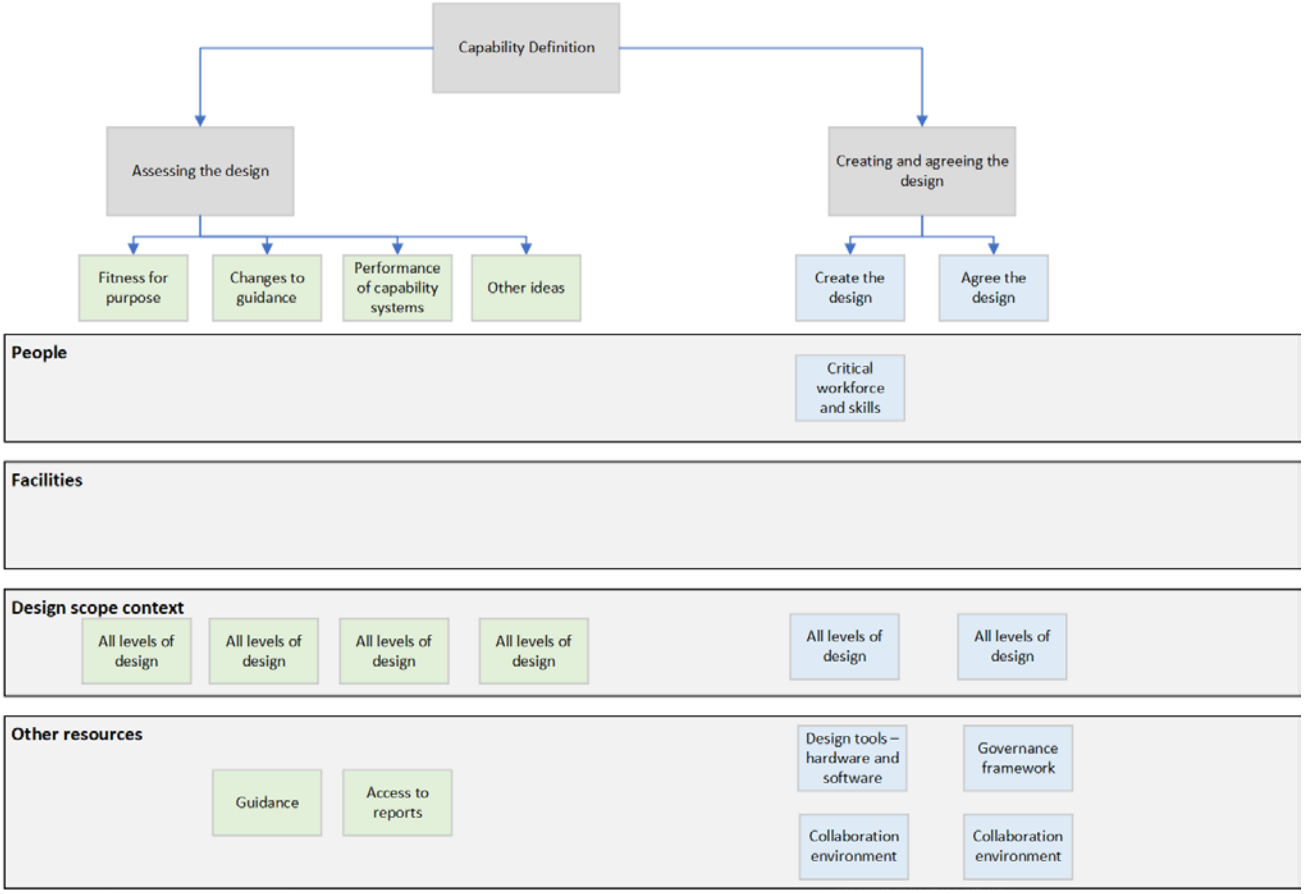

Figure 22: Considerations for the 'capability definition' component

Products

84. The key outcome from this component is the means to manage the S-IB as Products.

85. The elements involved in a framework to manage Products include:

a. Assessments of whether the Product is fit for purpose, in that it can still perform to the agreed specification in support of the desired capability effect

b. Assessments of whether the assets continue to perform within tolerance – to the agreed specification – and that any variances in expected performance[9] are assessed against the design

c. Assessment of change requests from operators

d. Assessment of alternative assets that can achieve the same function as the existing assets

e. Assessment of updated guidance on the scope and life of Products, and the associated assets

f. Contract management for sustaining activities.

g. A training framework so that Product Managers can train operators and maintainers

86. Inherent in this activity is the ability to communicate relevant information regarding the Products. Examples of external stakeholders and their use include:

a. Operators for evolving knowledge of how to use Products in the changing capability environment and evolving knowledge on how the Product effects the environment

[9] Expected performance includes defect rates and obsolescence considerations.

b. Maintainers for evolving knowledge of how to maintain Products in the changing capability environment and feedback on the efficiency or effectiveness of extant maintenance processes

c. Capability Managers for insight on how Products continue to address strategic and operational needs

d. Industry, and in particular Australian Industry, for strategic Business and Industry Capability Development in support of Products

e. Delivery agencies and project teams for capability delivery

f. Engineers for guidance on risks and issues relating to capability systems

87. The following figure illustrates the resources required to achieve the Product management component outcomes.

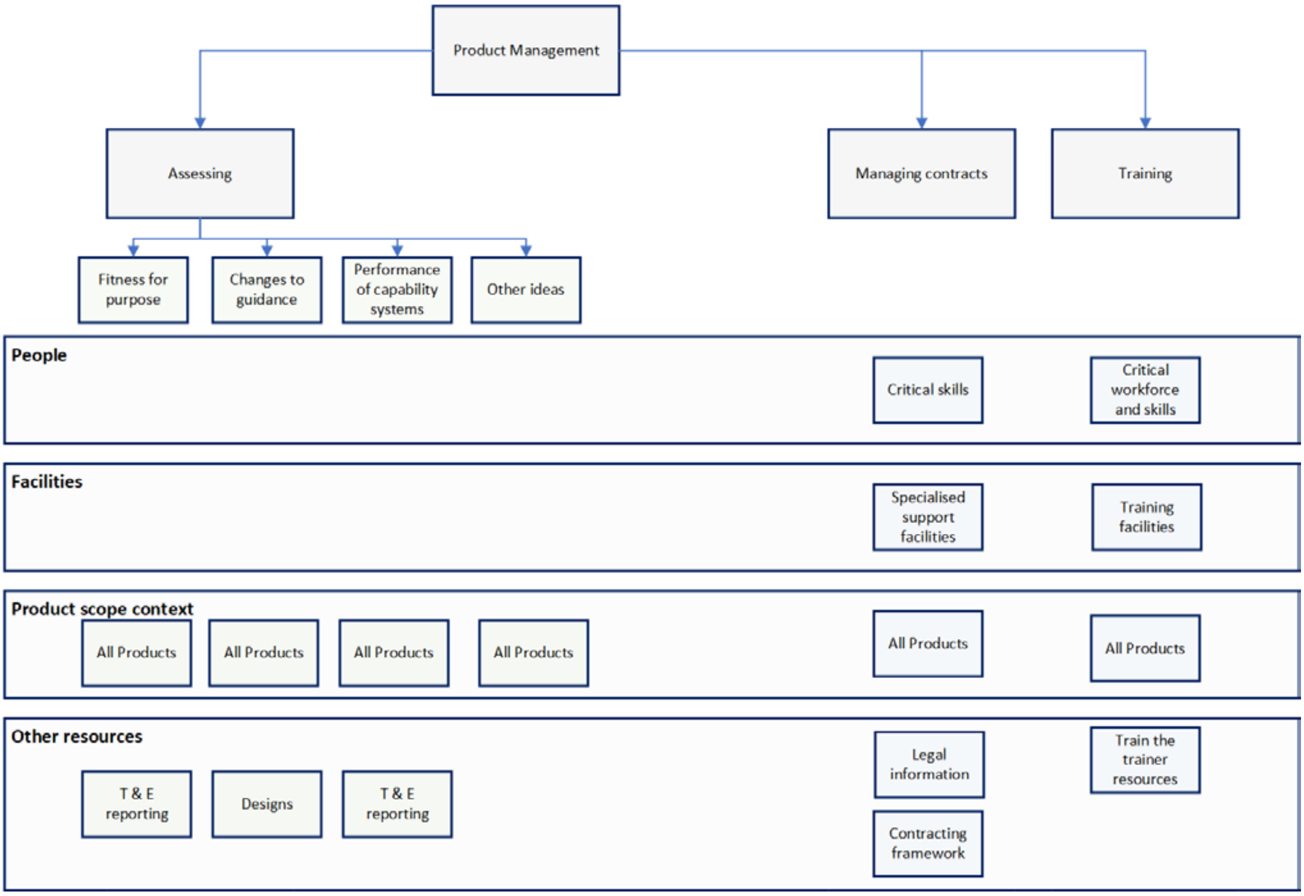

Figure 23: Considerations for the 'Products' component

Change activities

88. The key outcome from this component is the means to prioritise, initiate and coordinate change activities. These change activities are intended to transition capability systems from the extant form to the agreed design.

89. The underlying assumption is that the need for change is driven from the capability design and that change activities do not drive their own requirements. In addition, the CCDS facilitates and initiates change activities, but it does not perform the change activities themselves.

90. The elements involved in change activities are:

a. Acceptance or approval of the changes required

b. Assessments of the priority or achievability of the changes required, including technical and financial viability

c. Management of the activities that create the changed Products

d. Management of the activities that transition the changed Products to operational use, including training of operators and maintainers

e. Documentation of the realised changes to be incorporated into the capability design.

91. The simplicity of the statement "management of the activities that create the changed Products" belies the known complexity of the various level of changes. The CCDS must categorise the recommended changes accordingly and facility the appropriate path.

a. Some changes will require higher committee or Government approval and may follow a formal Defence Project process

b. Some changes will fit within the remit of existing programs but will still require formal project and engineering methodologies

c. Some changes will fit within the remit of existing programs and can be realised through the engineering and sustainment frameworks.

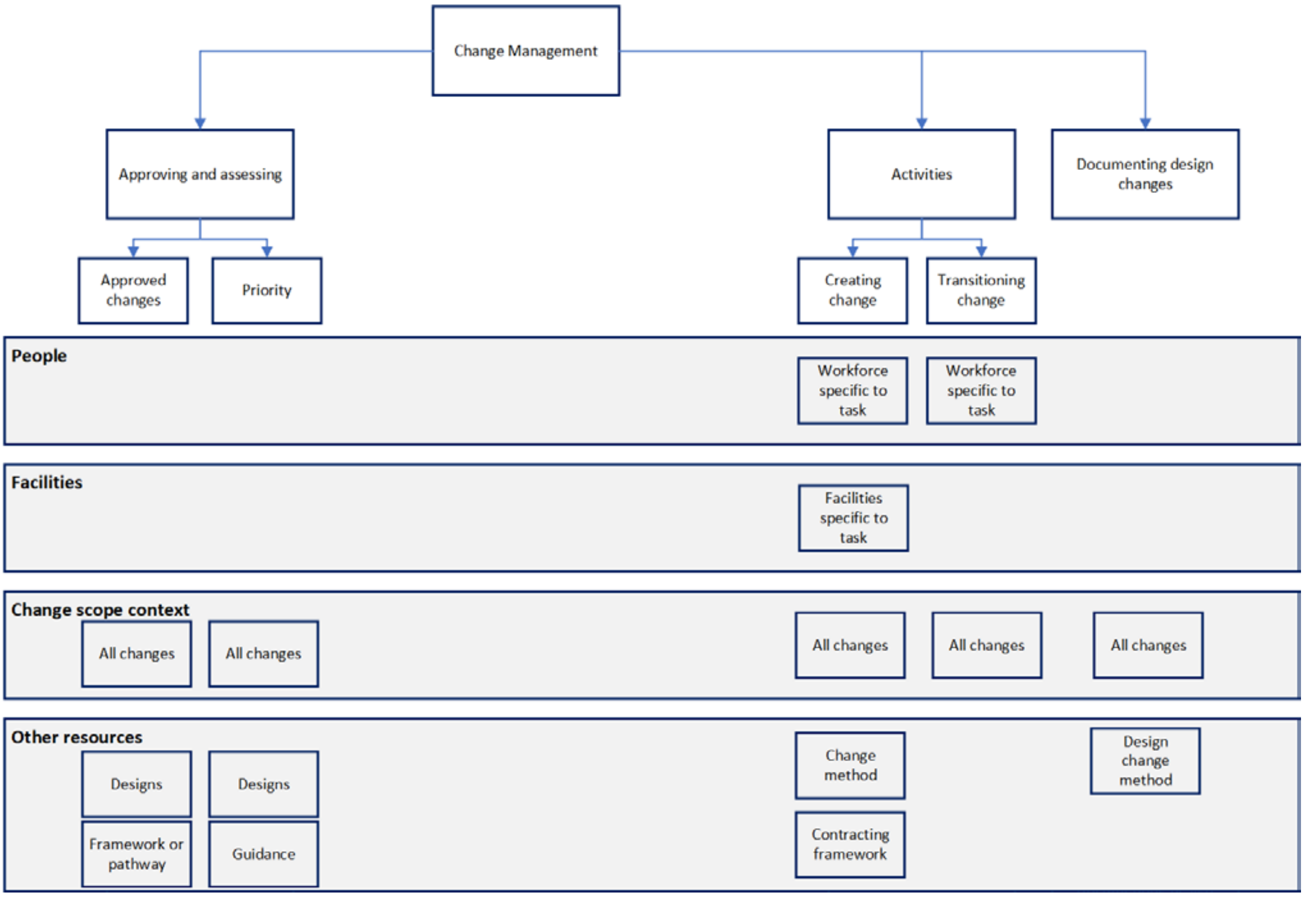

Figure 24: Considerations for the 'change activities' component

Evolution and innovation

92. The key outcome from this component is a range of research and development activities intended to improve knowledge of systems or effects. That improved knowledge may be in the form of prototype or proof of concept systems.

93. Another outcome from this component is an evolution path and mechanism to ensure capability systems and fundamental inputs to the capability will continue to match the changing needs.

94. The elements involved in evolution or innovation are:

a. Theoretical research to identify future concepts, based on papers or available information

b. Review of emerging Products or technology

c. Acceptance and assessment of ideas from stakeholders for evolution or innovation

d. R&D to develop concepts, building the pool of papers and available information

e. R&D to prove concepts, building a foundation for emerging technology

f. R&D to mature concepts, building a pathway to productisation and manufacture

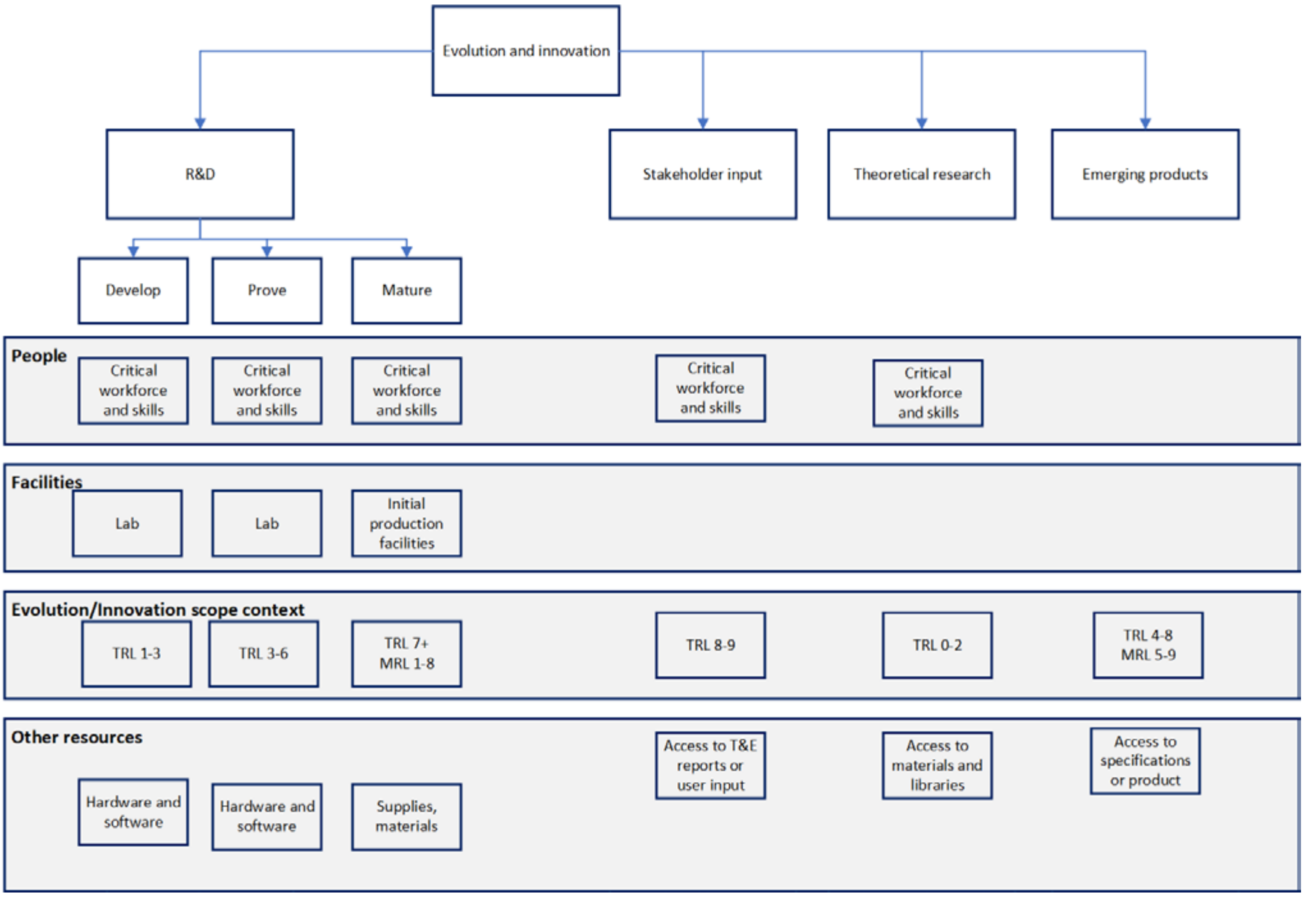

Figure 25: Considerations for the 'evolution and innovation' component

Funding and resources

95. The key outcome from this component is the funding or resources required for delivery of capability systems or the delivery of capability effects.

96. The elements involved in funding and resources are:

a. Business cases to present to funding agencies

b. Need statements for ongoing funding, for both acquisition and sustenance activities.

c. Contract management to ensure that funding flows and expected resources are available

d. Accounting and payment systems (financial management systems) to manage the funding and resources to ensure confidence of value for money and risk management

97. The complexity of the capability program results in multiple streams of each element. Multiple funding sources and financial management systems will be used. While individual contracts will be managed within a single framework, multiple contract management frameworks are required for the variety of contract types that will be used.

98. The funding scope includes:

a. Acquisition of capability systems

b. Support to capability systems

c. Operation of the CCDS

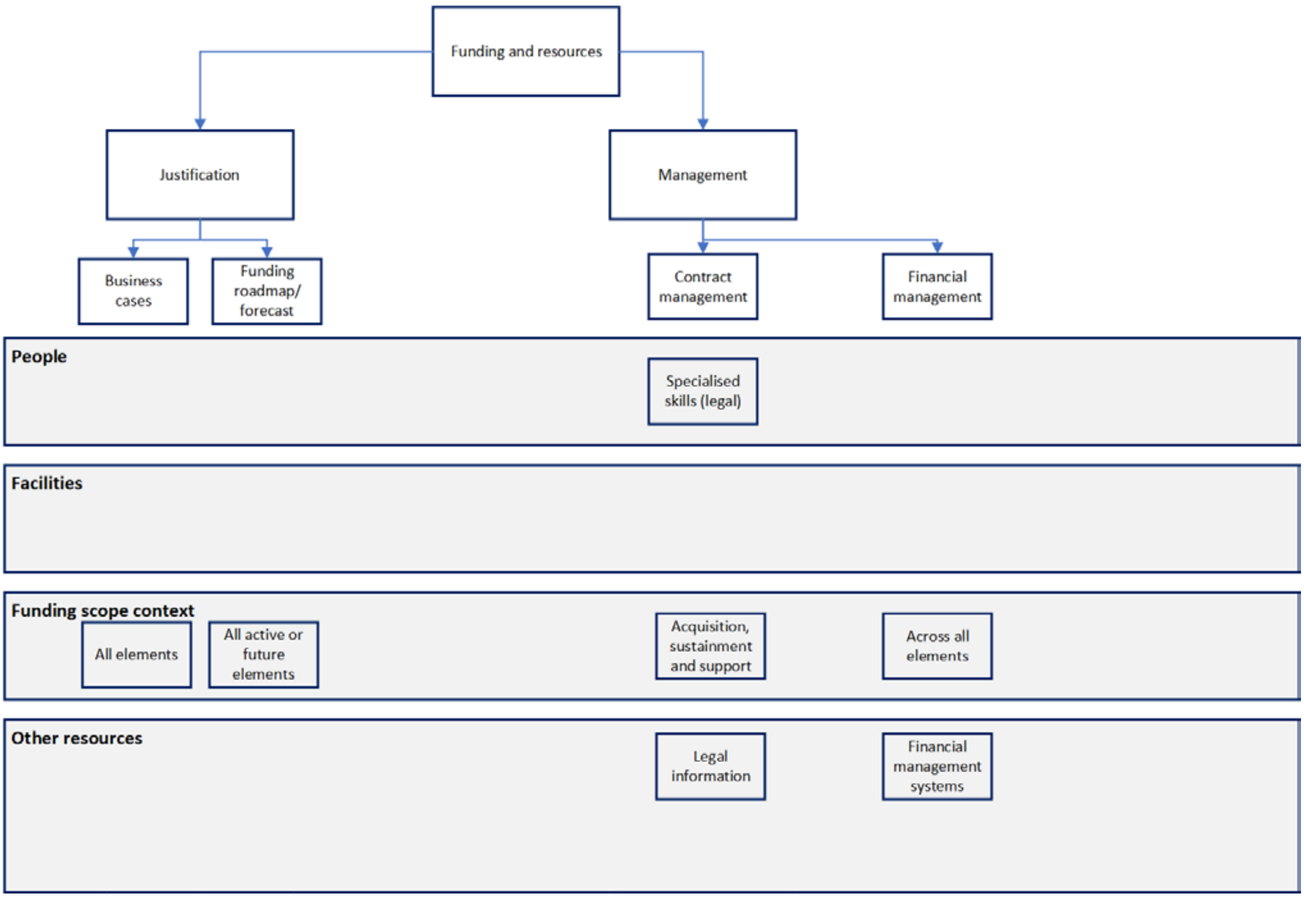

Figure 26: Considerations for the 'funding and resources' component

CCDS components and the architecture

99. The previous sections identify the components of the CCDS. This section places the description in more formal architectural terms to ensure architectural compliance with the capability architecture. In addition, consistent with the architecture framework, this section places the elements described previously in the context of FIC to allow the acquisition of the CCDS.

100. At the broadest level, this concept document addresses the current capability against an evolving threat environment. This addresses an Effect, through Measurable Characteristics. The following table categorises elements relating to the various components and matches these against the FIC and the capability architecture.

Table 1: FIC, elements and capability architecture elements

FIC[10]	CCDS elements	Architecture elements
	[UTE] – Understanding the environment [CD] – Capability Definition [PM] – Product Management [CM] – Change management [E&I] – Evolution and innovation [F&R] – Funding and Resources	
Command and management	[UTE] Guidance on reporting [CD] Governance framework for agreeing the design [PM, CM] Contracting framework [CM] Change method such as project or engineering framework [CM] Method for changing the design	Effect (guidance) Activity (process, framework)
Major systems	[UTE] Systems for H/SITL [CD] Design tools [CD] Collaboration environment [E&I] Hardware and software for R&D [F&R] Financial management systems	Product
Facilities and training areas	[UTE] Secure facilities for assessment and simulation, including H/SITL activities [UTE] Facilities and training areas for graduated exercises [PM] Training facilities, could be LVC [PM] Some capability elements will require specialised support facilities [CM] Some projects will require specialised facilities to create and realise change [E&I] Laboratories to develop and prove research [E&I] Initial manufacturing facilities	Product (facilities)

[10] At the time of drafting, Data had not been added to the FIC categories.

FIC[10]	CCDS elements	Architecture elements
Personnel	[UTE] Specialists to assess the threat environment [UTE] Specialists to simulate the threat environment [UTE] Specialists to perform H/SITL testing and evaluation [CD] Hard-to-get architects and system/capability designers [PM] Contract managers for Product support [PM] Training developers [CM] Project teams to create change [CM] Transition teams to transition/realise change [E&I] R&D specialists across the fields of develop and prove research [E&I] R&D specialists to mature/bring to production research [E&I] Research specialists for theoretical research [F&R] Contracting and legal skills	Resources (stakeholders)
Organisation	As required	
Collective training	Graduate exercises for training, operational evaluation, and test and evaluation purposes	Activity
Industry	As required	
Supplies	[UTE] Background information for assessments [UTE] Algorithms and parameters for simulation [UTE] Algorithms and parameters for H/SITL [UTE, CD] Operational evaluation reports [CD] Higher guidance [PM, E&I] T&E reporting [PM] Designs to be used in Product Management [PM, F&R] Legal information to support contract management [PM] Train the trainer resources [E&I] Supplies and materials for initial production [E&I] Specifications or actual product for emerging products [E&I] Research papers or research libraries for theoretical research.	Business Items
Support	[UTE] Support resources for graduated exercises	Activity