Australian Government

dta

Digital Capability Assessment Process (DCAP)
A guide for agencies

Contents

Australian Government Digital and ICT Investments – DTA Oversight

The Digital Transformation Agency (DTA) provides strategic advice, policy leadership and assurance to the Australian Government (the Government) on its digital and ICT investments to help drive the digital transformation of public services.

The DTA is responsible for managing strategic coordination and oversight functions for digital and ICT investments across the initiative life cycle.

The DTA delivers this by:

- providing advice to agencies developing business cases, new policy proposals, and Cabinet Submissions, to ensure they align and comply with whole-of-government digital and ICT policies, priorities, and standards

- providing advice to the Government when deciding on new digital and ICT investment policy proposals

- ensuring agencies plan for assurance with agreed plans which are then overseen during delivery

- collecting regular project performance reports from agencies and providing advice to the Government on the overall health of its digital and ICT investment portfolio.

The Digital Capability Assessment Process (DCAP) - A guide for agencies

The DCAP (formerly known as the Digital Capability Standards [DCS]) is the process the DTA applies to contest digital proposals coming forward in the Budget process to ensure they are aligned with Cabinet-agreed digital policies and standards.

This guide is used to assist agencies in understanding the context and purpose of the DCAP, and to guide agencies in using the DCAP Assessment Tool with further information on each digital and ICT policy and standard.

Whole-of-Government Digital and ICT Investment Oversight Framework (Investment Oversight Framework)

The Australian Government has a Whole-of-Government Digital and ICT Investment Oversight Framework (Investment Oversight Framework) to manage its digital and ICT investments. Overseen by the DTA, the Investment Oversight Framework is a six-stage, end-to-end framework providing a way for the Government to manage digital investments across the entire initiative lifecycle. The Investment Oversight Framework was endorsed by Government as part of the 2021-22 Mid-Year Economic Fiscal Outlook (MYEFO).

Agencies are required to work with the DTA to ensure all digital and ICT investments are planned, developed, and implemented in accordance with government requirements, and aligned to the Investment Oversight Framework.

Digital and ICT Workforce Considerations

The APS is experiencing shortages in digital and ICT roles. Demand for digital and ICT job family roles is expected to have a strong to very strong growth in the APS as well as the within the broader economy over the next 5 years. When planning your digital and ICT investment proposal you should consider the workforce capacity and capability to achieve the outcomes of your investment. Consideration should be given to the skills required and their availability in the market and how this might impact project timelines, deliverables and on-going workforce needs post-project. For more information on how to plan for your workforce visit the APSC's Workforce Planning Resources.

6 Stage Process

1. **Strategic Planning** defines the Government's digital and ICT investment portfolio, its future objectives and identifies capability gaps.

2. **Prioritisation** prioritises, plans, and advises on investments to deliver on the Government's digital and ICT objectives.

3. **Contestability** assesses compliance with whole-of-government digital and ICT policies as part of ensuring proposals brought forward for government consideration are robust.

4. **Delivery Assurance** provides assurance to the Government that investments are on-track to deliver expected benefits.

5. **Sourcing** ensures Government obtains the best value for money from digital and ICT investments.

6. **Operations** is a direct feedback loop of the successes and areas to improve the Australian Government Architecture (AGA) and the content that guides agency investments in digital.

Investments subject to the Investment Oversight Framework

The Investment Oversight Framework applies in principle to all government digital and ICT investments which are defined as:

- Investments that use technology as the primary lever for achieving expected outcomes and benefits. This includes investments that are:

  - transforming the way people and businesses interact with the Australian Government

  - improving the efficiency and effectiveness of Australian Government operations, including through automation

The Investment Oversight Framework applies where the digital and ICT investment:

- is brought forward by a non-corporate Commonwealth entity and, where specifically requested by the Minister responsible for the Digital Transformation Agency, a Corporate Commonwealth entity; and

- involves ICT costs[1]; and

- is being brought forward for government consideration as a new policy proposal.[2]

Compliance with the Budget Process Operational Rules

All policy proposals must have authority from the Cabinet or the Prime Minister[3] and must comply with the Department of Finance's Budget Process Operational Rules (BPORs) to come forward for consideration. The BPORs include the DTA's digital and ICT oversight function in the Budget and MYEFO process. As the BPORs is not in the public domain the below information summarises the requirements under the BPORs.

For all digital and ICT investment policy proposals, agencies must consult the DTA early and as part of the DTA prioritisation process to:

- ensure that the digital elements of their policy proposal align and comply with relevant digital and ICT whole-of-government policies; and

- determine if the policy proposal is subject to the ICT Investment Approval Process (IIAP).

Agencies must receive correspondence from the DTA that they have provided sufficient information to the DTA before their policy proposal is being considered by Government.

Agencies are also required to provide any requested information on any ICT policy proposal or project to the DTA to support its role in overseeing projects throughout the initiative life cycle.

---

1   All new policy proposals (post july 2021) with ICT costs are subject to the Contestability (Stage 3) and Delivery Assurance (Stage 4) stages of the Investment Oversight Framework. For clarity, different thresholds and eligibility criteria apply for the ICT Investment Approval Process and the annual prioritisation process (Stage 2). Additional information is available on request from the DTA.
2   The DTA and the Department of Defence are applying the Investment Oversight Framework in a way that avoids duplicating Defence's established, comparable, and effective strategic planning and decision-making process under the Defence Integrated Investment Program (IIP) or the application of standards and policies compromising warfighting or coalition requirements.
3   A delegate acting on behalf of the Prime Minster may provide or alter authority to bring forward policy proposals.

The Digital Capability Assessment Process

The Digital Capability Assessment Process (DCAP) is a set of whole-of- government digital and ICT policies and standards that all new digital and ICT investment proposals will need to demonstrate a level of alignment and compliance with, prior to consideration by Government.
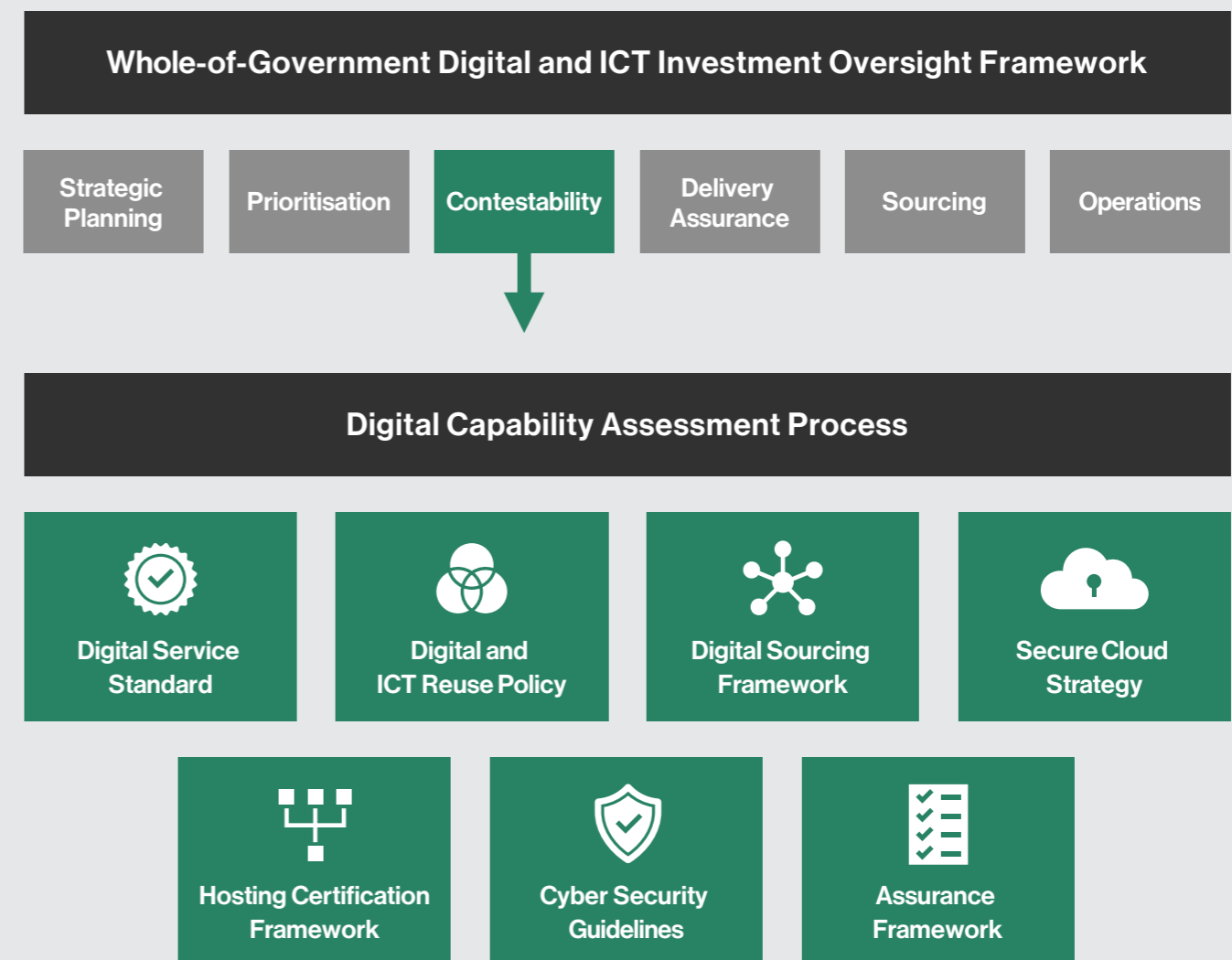
The purpose of the DCAP is to ensure all digital and ICT investment proposals are robust, align to common minimum standards, and include fit-for-purpose assurance, to meet the Australian Government's digital and ICT objectives. The DCAP underpins the Contestability (Stage 3) of the Investment Oversight Framework.

The DTA will use the DCAP to consistently assess all new digital and ICT investment proposals to advise Government.

The DTA assessment may determine whether the proposal goes forward for Government consideration.

Agencies should engage the DTA at the earliest opportunity when preparing digital and ICT investment proposals, to ensure there is sufficient time for the DTA to work with agencies to ensure their proposals align and comply with relevant whole-of-government digital and ICT policies and standards.

Where the Digital Capability Assessment Process fits within the Investment Oversight Framework

Whole-of-Government Digital and ICT Investment Oversight Framework					
Strategic Planning	Prioritisation	Contestability	Delivery Assurance	Sourcing	Operations

Digital Capability Assessment Process			
Digital Service Standard	Digital and ICT Reuse Policy	Digital Sourcing Framework	Secure Cloud Strategy
Hosting Certification Framework	Cyber Security Guidelines	Assurance Framework	

DCAP Policies and Standards for Budget 2023-24

As part of the 2023-24 Budget process, Government requires that all digital and ICT investment proposals comply with the following whole-of-government digital and ICT policies and standards (DCAP Areas):

Digital Service Standard – The Digital Service Standard ensures that government services are designed in a human centred way. Agencies must assess and comply with the principles of the DSS to ensure continuous improvement opportunities in support of effective project delivery.

Digital and ICT reuse policy – The Digital and ICT Reuse Policy ensures a whole-of-government focus on reuse of digital and ICT capabilities. Reuse also incorporates elements of the Australian Government Architecture, which is currently in development.

Digital Sourcing Framework – The Digital Sourcing Framework and the four associated digital sourcing policies ensure government buyers source digital products and services that enable a modern digital government.

Secure Cloud Strategy – The Secure Cloud Strategy aims to increase the take-up of cloud services by Commonwealth agencies. It outlines the requirements and security controls for Commonwealth agencies to assist in assessing cloud service providers and cloud services.

Hosting Certification Framework – The Hosting Certification Framework is integral to protecting Australian Government systems and the data they hold. It provides guidance to Australian Government agencies enabling them to identify and source hosting services that meet enhanced privacy, sovereignty, and security requirements.

Cyber Security Guidelines – The Cyber Security Guidelines in the DCAP work to ensure government digital services and systems meet minimum cyber security standards based on technical guidelines published by the Australian Cyber Security Centre (ACSC).

Assurance Framework – The Australian Government's Assurance Framework helps provide Ministers and other key stakeholders with confidence that assurance is being applied effectively to support successful delivery of digital and ICT investments.

Candidate Policy Pilot: Digital Investment Benefits Management Domain – Benefits management enables the identification, measurement, planning, and realisation of project benefits through a structured approach and helps provide program sponsors and Government with confidence that Digital and ICT projects will realise their intended outcomes.

How to apply the DCAP

To assist agencies in complying with the DCAP, the DTA has developed the *DCAP Assessment Tool* to:

- raise awareness of whole-of-government digital and ICT policies and standards;

- enable agencies to substantiate how their proposal aligns to whole-of-government digital and ICT policies; and

- enable the DTA to assess digital and ICT proposals in a consistent, coordinated, and robust manner, to then provide advice to inform Government consideration of the proposal.

How to use the DCAP Assessment Tool

The *DCAP Assessment Tool* (the Tool) is an Excel workbook for agencies to complete when submitting a new digital and ICT investment proposal. When completing the Tool, agencies are required to consider how their new digital and ICT investment proposal aligns with the seven DCAP Areas.

Each DCAP Area is underpinned by detailed criteria describing key requirements agencies must consider in designing digital and ICT proposals. Each criterion provides detailed guidance on how to demonstrate alignment.

Agencies must describe and provide evidence to substantiate how their proposal aligns with each DCAP Area. The suitability of evidence is based on the extent it answers the criterion.

The Tool contains the following worksheets:

- **Instructions** – to step the user through how to complete each worksheet.
- **A. Proposal details** – to identify the proposal.
- **B-I Seven DCAP Area worksheets** – to consider and substantiate how the proposal aligns with each DCAP Area.
- **DCAP Assessment (for internal use)** – records the outcome of the DTA assessment of the proposal.

When completing the Tool, please note that:

- Agencies must provide a response to all DCAP Areas and criteria. Where the agency believes a particular DCAP Area is not applicable, or is not able to address a particular DCAP Area, they must use 'no' in the relevant drop-down box and provide a detailed explanation.
- If the DTA considers the DCAP Area is applicable, the agency will be required to provide a full response and supporting information.
- If a DCAP Area is not relevant to a proposal, it is the agency's responsibility to notify the DTA of any changes to the proposal that may alter that assessment.
- Where a proposal materially changes following a review by the DTA which then brings a previously not applicable DCAP Area in-scope, this area will need to be assessed by the DTA.
- The DTA may, at its discretion, advise the agency of specific response requirements, including but not limited to an alternate form of the tool.

How is the DCAP Assessed by the DTA

The DTA will assess the claims made against each DCAP Area criterion along with the evidence provided.

The DTA will provide feedback to the agency against each DCAP Area in its DCAP Assessment. Engaging with the DTA at the earliest opportunity is strongly recommended to ensure there is sufficient time to address areas where alignment has yet to be achieved.

The DTA will use the DCAP Assessment to advise the Government on the DTA position on the proposal.

Agencies should provide their DCAP Assessment to the DTA as soon as suitable evidence can be supplied.

Further Information

Further information on each of the DCAP Areas can be found in the next section on DCAP Policies and Standards – Factsheet.

This Guide will be updated periodically in response to agency feedback.

For the most current version of this Guide, or if you need additional information, please contact the DTA at investment@dta.gov.au.

DCAP Policies and Standards – Factsheets

1. Digital Service Standard (DSS)

Overview

The DSS is a set of best-practice principles for designing and delivering government services. These principles are informed by best practice human-centred design (HCD) frameworks and concepts.

These principles incorporate ideas from leading digital governments and jurisdictions around the world including in the United Kingdom, Canada and New South Wales.

The need for user-driven design is central to the Australian Government's digital transformation aspirations. It underpins delivering a digital government that meets and exceeds the expectations of Australians as outlined in the Digital Government Strategy.

The DSS aims to help agencies meet a minimum standard and build toward better practice standards of user-driven design by assessing against and providing guidance on:

- identifying user groups and their needs

- understanding user experience, the context (ecosystem) and — when the end users are the public — taking a life event perspective

- co-designing future states to balance desirability, feasibility, and viability

- measuring and evaluating user needs and experience for continuous improvement

Assessment Requirements

The DSS must be applied to Australian Government Services that are:

- public facing; and

- owned by non-corporate commonwealth entities; and

- new informational or transactional services; and/or

- existing high-volume transactional services.

More information on the DSS is available on the DTA's website:

About the Digital Service Standard
Digital Transformation Agency
(dta.gov.au)

2. Digital and ICT Reuse Policy

Overview

The Digital and ICT Reuse Policy aims to reduce duplication of investment and long-term costs involved in digital and ICT delivery across government. It also helps drive lower build and run costs, increase speed and certainty of delivery, and provide more joined-up services for people and businesses.

Under this policy, agencies must consider three key requirements when designing, proposing, or delivering new government capabilities with a digital and ICT component or improving existing ones:

1. Reuse whenever possible – agencies must plan for and make use of any opportunities to reuse existing technology and architecture, business capability and process, procurement, information and data, skills, and capabilities within their agency and across government.

2. Design and build for reuse – if agencies can't reuse an existing solution, they must ensure anything new they create can be reused by other agencies.

3. Enable reuse by others – agencies must ensure anything new they propose to create is shared for others to reuse unless there's a good reason not to. There should be evidence that agencies have consulted the DTA to ensure reuse opportunities are not already available across the Australian Public Service (APS).

Interaction with the Australian Government Architecture

Reuse opportunities may also be informed by the Australian Government Architecture (AGA).

As the AGA is released iteratively it will provide designs and patterns for reuse for a growing number of capability areas of Government operation and service. Prior to Government agreement of the AGA policy, the AGA should only be referred to in relation to the application of patterns and designs for reuse. Agencies should contact the Architecture team (architecture@dta.gov.au) if they are unsure of where their capability might sit within the DTA model.

More information is available on the DTA website:

Whole-of-Government Architecture Digital Transformation Agency (dta.gov.au)

Assessment Requirements

Where agencies are developing a new capability that does not yet exist in government, they must consider how that capability could be reused in the future to help the APS achieve desired outcomes more efficiently.

These considerations must be made at the beginning of an investment before work starts on capability build or the contracting of providers. Agencies should consider reuse as a principle for all investment activities.

The DTA will assess all Digital and ICT proposals against the policy. This includes proposals to change or create all types of government services. More information on the Digital and ICT Reuse Policy is available on the DTA's website:

Digital and ICT Reuse Policy Digital Transformation Agency (dta.gov.au)

3. Digital Sourcing Framework

Overview

Sourcing (including procurement) plays an important role in the successful delivery of ICT and digital investments. It covers every part of the acquisition, sustainment, and disposal of an investment, from identifying a need to managing delivery, to end-of-life arrangements.

The Digital Sourcing Framework is a set of principles, policies, and guidance that guides agencies on how to buy digital products and services on behalf of the Australian Government. It provides benefits for buyers and sellers, with policies aimed at reducing procurement risk and gives better access to small and medium enterprises offering innovative agile solutions. This also introduces scope for innovation and a wider range of solutions by widening the supplier base.

The policies within the Digital Sourcing Framework are:

- Consider First
- Digital Panels
- Fair Criteria
- Contract Limits and Reviews

To meet these requirements, agencies must demonstrate suitability against the four Digital Principles of being Secure, Effective, Connected and Sustainable.

Assessment Requirements

All submissions that include a digital sourcing component will be assessed against the Digital Sourcing Framework. The degree and approach of assessment may vary as the sourcing arrangements become clear through the process. For example, in New Policy Proposals, knowledge of the policies and the procurement plan approach should be targeted as further detailed information, such as contractual arrangements, may not be known. The assessment should be more comprehensive at the second pass business case development.

More information on the Digital Sourcing Policy is available on the DTA's website:

Policies
Digital Transformation Agency
(dta.gov.au).

4. Secure Cloud Strategy

Overview

The Secure Cloud Strategy is designed to help agencies transition to cloud-based services while maintaining appropriate security and functionality. The strategy was developed with reference and alignment to the following existing guidelines:

- The Australian Government Protective Security Policy Framework (PSPF) which assists Australian Government entities to protect their people, information, and assets both at home and overseas. The PSPF was developed by the Attorney-General's Department (AGD) and sets out government protective security policy and supports entities to effectively implement the policy across the following outcomes: security governance, information security, personnel security, and physical security.

- The Information Security Manual (ISM) is an information control framework that can be used to harden and protect cloud-based services. The ISM was developed by the Australian Cyber Security Centre (ACSC) and provides guidelines and principles for agencies preparing or undergoing the transition to the cloud.

Using cloud-based services can deliver the following benefits:

- increases the speed of delivering new platforms
- allows for continuous improvement
- provides easier access to services
- reduces the effort needed for maintenance and allow agencies to focus on improving service delivery
- provides a shared risk model to mitigate cyber risks

Assessment Requirements

All proposals will be assessed against the Secure Cloud Strategy. The following principles must be considered:

- make risk-based decisions when applying cloud security
- design services for the cloud
- use public cloud services by default
- use as much of the cloud as possible
- avoid customisation and use cloud services as they come
- take full advantage of cloud automation practices
- monitor the health and usage of cloud services in real time

More information on the Secure Cloud Strategy is available on the DTA's website:

Secure Cloud Strategy Digital Transformation Agency (dta.gov.au)

5. Hosting Certification Framework
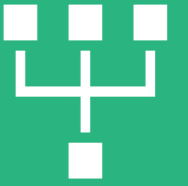
Overview

The Whole-of-Government Hosting Strategy provides a whole-of-government approach for hosting services used by the Australian Government. This strategy provides policy direction and guidance for different hosting service models, including agency hosted, managed service provision, and cloud-based software-as-a-service.

The Hosting Certification Framework (HCF) has been developed to operationalise the principles outlined in the whole-of-government Hosting Strategy, and to support the secure management of government systems and data. It supports the Government's commitment to privacy, security, and resilience, while improving the delivery of government services.

The HCF assists agencies to mitigate supply chain and data centre ownership risks and enable them to identify and source appropriate hosting and related services.

The DTA certifies and maintains a list of all certified hosting providers that offer certified hosting services to government.

Assessment Requirements

All proposals delivering digital / data capabilities will be assessed against the HCF. All hosting procurements should use Certified Service Providers. Australian Government entities continue to have the autonomy to select the best hosting arrangements to suit their requirements.

The DCAP assessment will consider two elements:

- Assessment of the sensitivity or classification of the data.
- Compliance with the HCF for procuring a Certified Provider.

The following HCF principles apply to Australian Government hosting arrangements:

- Hosting arrangements must be designed to ensure resilience and business continuity.
- Hosting arrangements must be founded on robust, risk-based assessments to ensure data sovereignty and supply chain integrity.
- Existing policies and certification processes should be used where appropriate.
- Where common hosting requirements are identified across the APS, centralised arrangements should be accessible and leveraged.
- Government entities continue to have the autonomy to select the best hosting arrangements for their requirements.

From 30 June 2022, all new and extensions to existing contracts for hosting services should be with a Certified Service Provider(s). Visit the HCF website for guidance on procurements involving a provider who is not yet certified.

More information on the HCF is available on the DTA's website:

Hosting Certification Framework Digital Transformation Agency (dta.gov.au).

6. Cyber Security Guidelines

Overview

This DCAP Area, based on existing Australian Cyber Security Centre (ACSC) technical advice and guidance, identifies key standards, practices and procedures that are designed to harden and protect technology and information from information security threats.

The DTA's advice on this DCAP Area focusses on ensuring agencies adhere to relevant guidance in a manner which promotes and maintains the security, resilience, and reliability of information and technology assets.

The set of Cyber Security Guidelines agencies must apply will continually evolve, as they are not owned or maintained by the DTA. The list below is not exhaustive but should provide an appropriate guide for agencies to consider, along with their own internal Cyber Security capabilities.

Information Security Manual

The Australian Cyber Security Centre (ACSC) produces the Australian Government Information Security Manual (ISM). The manual provides a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threat.

Assessment Requirements

Cyber security is a critical enabler of all digital capabilities. It is expected that all proposals will be able to provide some level of response around how they will ensure the proposed solution will be secure. The level of depth will be dependent on the particulars of each proposal and the stage of its development.

The DTA is required to assess all proposals against guidelines published by the ACSC including the ISM. These guidelines are owned and managed by the ACSC. The DTA's role extends only to ensuring proposals have sufficiently demonstrated an intent to comply. Where agencies need clarification on ACSC guidelines, queries should be directed to the ACSC:

www.cyber.gov.au and

asd.assist@defence.gov.au

7. Assurance Framework

Overview

Under its mandate, the DTA is responsible for providing Ministers, the Secretaries' Digital and Data Committee, and other key stakeholders with confidence that assurance is being applied effectively to support successful delivery of digital and ICT investments.

This assurance oversight is centred on the Australian Government's Assurance Framework for Digital and ICT investments (the Assurance Framework). The Assurance Framework sets out minimum assurance requirements for in-scope investment proposals. The Assurance Framework also links to a tiering model which ensures fit-for-purpose assurance arrangements are prepared which align with the risk profile and scope of each proposed investment. Should the proposal be agreed, these arrangements are required to be calibrated as delivery continues to ensure they remain fit-for-purpose.

The Assurance Framework's goal is to maximise the value of assurance to successful delivery of digital and ICT investments, drawing on global experience and learnings. To achieve this, the Assurance Framework aims to:

- Achieve carefully planned, targeted, and fit-for-purpose assurance for all in-scope investments, with assurance information applied effectively to improve the quality of decisions by Senior Responsible Officials and governance boards.

- Maximise the value of assurance in supporting successful delivery, including through ensuring agreed recommendations are implemented in a timely manner.

- Realise clear escalation processes which help agencies take decisive early action to recover investments at higher risk of not delivering expected benefits.

- Achieve a steady flow of reliable information on the condition of major investments for central agencies, supporting reporting and analysis for Cabinet and Ministers on the investment portfolio.

Importantly, the Assurance Framework ensures agencies remain accountable for leading the delivery of their proposal. The Assurance Framework is designed to complement and build on existing Australian Government assurance processes including Gateway Reviews.

Assessment Requirements

All digital and ICT investments that meet the eligibility criteria of the Investment Oversight Framework (see page 5) are required to develop and agree to fit-for-purpose assurance requirements under the Assurance Framework. This occurs as part of the broader DCAP assessment process.

Requirements under the Assurance Framework differ depending on the tier of an investment with the tier determined by the DTA.

The following key principles for good Assurance should be considered when developing proposals:

- Plan for assurance

- Drive good decisions

- Expert-led and independent

- Culture and tone at the top

- Focus on risks and Outcomes

More information on the Assurance Framework is available on the DTA's website:

Assurance
Digital Transformation Agency
(dta.gov.au)

More information

For more information about the DCAP, please contact the DTA's investment advisers by emailing investment@dta.gov.au