Australian Government
Department of Finance

Gateway Review Report
Mid-Stage/ Gate 5 Review

For: Digital Identity Program

To: Lucy Poole

This report is the property of the Digital Transformation Agency and may only be distributed or reproduced with the permission of the Senior Responsible Official with the exception of projects or programs that include an ICT component, where the report will be shared with the Digital Transformation Agency (DTA).

Entity name:	Digital Transformation Agency	
Program/Project name:	Digital Identity Program	
Review type:	Blended Mid-Stage and Gate 5 – Benefits Realisation Review	
Senior Responsible Official (SRO):	Lucy Poole	
Planning Meeting date:	Tuesday 22 November 2022	
Review Week dates:	Monday 12 to Friday 16 December 2022	
Date report provided to SRO:	Friday, 16 December 2022	
Date report provided to Assurance Reviews Unit:	Friday, 16 December 2022	
Review Team Leader:	**Name**	**Signature**
	s22 [redacted]	[redacted]
Review Team Member:	**Name**	**Signature**
	s22 [redacted]	[redacted]
Review Team Member:	**Name**	**Signature**
	s22 [redacted]	[redacted]
Review Team Member:	**Name**	**Signature**
	s22 [redacted]	[redacted]
Template version control:	November 2022	

This report has been prepared in accordance with the Australian Government's Gateway Review Process (Gateway) methodology as set out in *Resource Management Guide 106: Australian Government Assurance Reviews.*

The report summarises the findings and recommendations of the review team, which are based on information provided to the review team during the review process.

A copy of the report is provided to the Assurance Reviews Unit (ARU), Department of Finance at the conclusion of the review to identify lessons learned and evidence of best practice. Where a project or program includes an ICT component the report is shared with the Digital Transformation Agency (DTA). The report is not shared more broadly without agreement from the SRO. A copy may be provided to subsequent review teams as pre-reading material for future reviews.

Enquiries regarding the Gateway methodology should be directed to:

Assurance Reviews Unit
Department of Finance
One Canberra Avenue
FORREST ACT 2603
Email: s22 [redacted]@finance.gov.au

Version 223/20 T

Gateway Assurance Dashboard

Delivery Confidence Assessment

Rating

The review team finds that the overall delivery confidence assessment for the program at this point in time is **Green/Amber** Successful delivery of the program to time, cost, quality standards and benefits realisation appears probable however constant attention will be needed to ensure risks do not become major issues threatening delivery.

Factors Affecting Rating

Digital Identity is a critical national digital infrastructure and a fundamental enabler of secure government service delivery and the broader digital economy.

The Digital Identity Program (Program) has been complex, involving the consumption and use of large volumes of digital services data from disparate jurisdictional and Commonwealth systems.

The previous Government placed the Program in a “holding pattern” (sustainment) from July 2022. As a result, the DTA Program has de-emphasised program management functions that were not funded during this phase, noting that delivery partner agencies continued their own program management.

In the last 12 months the Program has been successfully operating in sustainment and has onboarded new clients (including the Western Australian Government) and additional services.

It has also been working with its stakeholders to develop policy options and to seek agreement (pending) to come forward in the 2023-24 Budget context, to establish Digital Identity as permanent arrangement in the Australian Government context with the potential to support whole of economy services.

The Program has domain expertise and experience in Digital Identity policy and has effectively considered the policy options and associated risks and impacts, demonstrating to the review team that is well placed to advise Government.

Since December 2021, stakeholders have observed positive improvements in the Program’s capability. There is also strong stakeholder support and engagement which provides greater confidence that a permanent technical solution can be delivered and administered, reflecting the green/amber rating.

Summary of Key Focus Area Ratings

Key Focus Area	Rating
Achievement of Outcomes	Amber
Stakeholders and End Users	Green
Governance and Planning	Green
Risk Management	Amber
Review of Current Phase and Operational Effectiveness	Green
Readiness for Next Stage	Amber

Summary of Findings

There has been strong growth in uptake by Australian citizens of myGovID since the last review.

While Digital Identity (DI) is a complex concept it presents opportunities to safeguard citizens' interactions with digital government services while at the same time providing convenience.

The recent incidents of cyber related breaches (Optus and Medibank) strengthen the need for digital safeguarding and the utilisation of a safe and secure digital identity.

While there are pockets of expertise, knowledge and expertise associated with DI in the Australian Government context is in short supply. It has also been difficult to message "in a simplified manner" the benefits and outcomes of DI.

Stakeholders interviewed strongly supported the Program and the need for a DI system with interoperability. However, there were differing views among the various stakeholders about legislation and regulation, including the charging model and timing for implementation of this.

Stakeholders provided positive feedback on improvements in governance and consultation, noting that senior executives (and Deputy Secretaries) from key agencies have been meeting to ensure policy and delivery outcomes are progressed.

There are a variety of emerging risks for the Program, including (non-exhaustive):

- Expansion and adoption of Digital Identity outside of the Commonwealth is dependent on legislation.
- Ongoing (permanent) funding, including the establishment of appropriate infrastructure is required to support this critical national asset.
- Fragmentation of digital identity responsibilities and accountabilities within the Commonwealth, impacts the Program's ability to coordinate and deliver the proposed and future digital identity policy reforms at pace.
- Not differentiating the options being put forward in the 2023-24 Budget context will make it difficult to assess the merits of each option based on investment, scope and benefits.

- There are also challenges moving at pace when there is a skill shortage across Australia, including the Australian Public service.
- Alignment with the recommendations from the myGov audit may present risks as well as opportunities.

It is acknowledged by stakeholders that the first order priority in future communications and messaging is "to keep citizens information safe and secure", with convenience being second.

The Program will need to be well prepared to ramp-up (planning and preparation) delivery to respond to any government decisions in the 2023-24 Budget context.

The Program delivery risk profile remains high until appropriate planning and preparation has been undertaken for the next phase of the Program.

Summary of Recommendations

The review team makes the following recommendations which are provided with an urgency category.

Item	Recommendation	Urgency
1	Prioritise setting a baseline and targets to measure and report benefits for Commonwealth agencies and establish processes for measuring and reporting on the endorsed option which may include economy-wide benefits.	Essential, Do by February 2023
2	On the basis that a preferred option is agreed by government, develop a communications campaign which emphasises safety and security and clarifies alignment of myGov and myGovID as part of the whole of government system.	Essential, Do by June 2023
3	Conduct a risk management workshop, incorporating internal and external stakeholders, to inform the development of the New Policy Proposal, and incorporate emerging risks into scenario planning for each proposed option.	Critical, Do Now
4	There should be a clear differentiation (separation) of each option in the NPP. Clearly articulate the proposed options so that these are differentiated and aligned to the benefits. Include appropriate communications messaging for each option.	Critical, Do Now
5	In anticipation of government directions and decisions on the MyGov Audit recommendations and related initiatives, be ready to "pivot". This should include the agility and flexibility to revise options and promptly prepare for Program design, delivery and coordination.	Essential, Do by March 2023
6	Subject to the agreed option in the 2023-24 Budget context, the Program should establish two governing committees to drive the whole of government (WoG) and whole of economy (WoE) benefits.	Essential, Do by June 2023
7	A Mid-Stage Review, in November 2023, would be to assess the Program's progress of delivering the agreed outcomes from the NPP (2023-24 Budget context).	Recommended

A summary of the previous review recommendations and actions taken can be found at Appendix B.

Definitions for the ratings provided for the Delivery Confidence Assessment, Key Focus Areas and Urgency Category are provided at Appendix F.

Appendices:

Appendix A. Gateway Assurance Plan.

Appendix B Previous Recommendations and Actions Taken.

Appendix C. Review Checklist.

Appendix D. List of Interviewees.

Appendix E. List of Documents Reviewed.

Appendix F. Assessment Rating Definitions.

Introduction

Program Description and Background

The outcomes and benefits of the program:

Identity verification has traditionally been done 'face to face'. Rather than a single identity card, Australia's system of identity verification relies on documents issued by roughly 20 government agencies across jurisdictions and the Commonwealth (for example, birth certificates, driver licences, passports and Medicare cards).

Digital Identity moves the identity verification process online. Digital Identity removes the hassle and insecurity in verifying information about a user. A common situation is one where a person needs to prove that they are over 18. Instead of needing to supply their entire identity document, they can simply use a Digital Identity to verify that they are 'yes, over 18'. Restricting the amount of information transmitted and stored is of immeasurable benefits to users. It also removes the need for users to supply all their information when only an attribute is needed (for example proving you are over 18 to drink and gamble).

A Digital Identity reduces the need to repeatedly re-verify identity within the one service. Having an authenticated and trusted identity gives both consumers and services confidence that people are who they say they are, meaning that more checks and cumbersome re-verifications are unnecessary. This principle applies across the whole-of-economy where Digital Identity is used - saving time while ensuring user's security.

Digital identities have the potential to streamline interactions across the economy, improve economic efficiency and lower transaction costs.

Currently, these benefits are only available for government services connected to the system and TDIF accredited Identity Providers. The passage of enabling legislation will allow these benefits to flow through to private relying parties (such as the banks, employment services and the housing sector) if they join the Government system. The legislation will also strengthen the enforceability of TDIF requirements (such as making the TDIF privacy safeguards legally enforceable), making it more attractive for businesses to seek TDIF accreditation for their users.

Identity data has also gradually shifted from being a commodity to being a liability. Organisations have realised that storing more data than is necessary is not worth the regulatory burden of storing it and the risk of potential data breaches. Large scale data breaches have also caused people to become mistrustful of organisations wanting to hold personal data. Therefore, solutions like Digital Identity have become significantly more attractive since it limits the amount of data shared across the economy.

The Digital Identity Budget 2020-21 Business Case sought funding to sustain previously delivered services, including an IP3 capability, develop Digital Identity Legislation, mature operational foundations, and expand the use of the Australian Government Digital Identity System (AGDIS).

The 2020-21 Budget was delayed to October 2020 and the authority for this business case was subsequently included under the Digital Initiative Business Package, a broad suite of initiatives to support the Government's COVID-19 response and the ongoing recovery of the economy. This shift in authority also adjusted and reprioritised the scope and potential benefits of the program.

Approved funding for the Digital Identity Program up until **30 June 2022** included:

- Integration with facial verification services (IP3).
- Finalisation of integration with myGov.

- The delivery of 14 additional government services.
- The onboarding of 5 states and territories and testing up to 3 new identity service providers.
- Independent privacy assurance by the Office of the Australian Information Commissioner (OAIC).
- Security and incident monitoring and a cyber security assessment by the ACSC.
- The development of primary legislation including a comeback in the 2020-21 MYEFO process with a strategy to introduce primary legislation.
- Gateway reviews by the Department of Finance to ensure the integrity of the program.
- Support to pass the IMS Bill as soon as possible to enable driver licences and other state-based identity documents.

The program entered sustainment on **1 July 2022**.

Approved funding for the program in sustainment extends to **30 June 2024** and covers the following

- recalibrating and consulting on the legislation and end state governance arrangements
- sustainment of existing services for current individual and business users
- onboarding of an additional five services
- enhancements to the AGDIS
- further accreditations under the TDIF
- pilots with states and territories.

s47C [redacted]

The policy context or need for the program:

In 2014, the Financial System Inquiry (FSI) found Australia's fragmented approach to identity verification drives up transaction costs in the financial system.

Prior to the FSI, Australia's private sector (led by the banks) tried to build a federated system but couldn't agree on the standards to adopt so that they could all connect to each other. The FSI recommended that the government step in to overcome this 'coordination failure' by developing a framework – this became the TDIF, which is now widely seen as the only workable framework for Digital Identity in Australia.

The TDIF specifies several roles against which organisations can be accredited to take part in the federated system. Because all organisations in the system are accredited against the same standards, services that want to use the system don't need to worry about which organisation is supplying which part of the service if they trust in the accreditation process. This is partly why this type of framework is sometimes called a *trust framework*.

Since the FSI, Digital Identity concepts have become more mainstream as organisations pursue the next phase of digital transformation.

Overseas, countries such as Denmark, Norway, Belgium, the Netherlands and France have successfully implemented national approaches to Digital Identity that have seen government and private sector services become more secure and accessible, having achieved over 30% adoption within 5 years. These high adoption rates are partly attributable to strong use cases across sectors, and a refined user-experience – though a large contributor to this adoption is that some countries mandate the use of Digital Identity to access government services (something that Australia has avoided).

For the system to work within the AGDIS, different agencies were asked to supply different services in the system:

- The Australian Taxation Office (ATO) was asked to create myGovID as the government's sole provider of identity verification services
- Services Australia was asked to supply the Identity Exchange (Exchange) to allow data to flow through the system
- Home Affairs upgraded verification services called the Document Verification Service and the Facial Verification Service
- The DTA was tasked with overseeing program implementation, legislative design and interim accreditation roles.

While there are only government agencies in the AGDIS at present, there is a desire to expand to include the private sector, to increase competition and consumer choice. It is mandatory to be TDIF accredited to supply identity services through the AGDIS, but other organisations can choose to apply to show their customers they meet the same strong exacting standards as those required by the government system.

Scope of the Review

This review will assess whether the agency (Digital Transformation Agency) is ready with its partner agencies to operate the AGDIS and finalise the remaining activities to ensure the System will operate as intended.

The review will also consider the DTA's approach and strategies to evolve the AGDIS to enable whole of economy benefits to be 'unlocked'.

Specifically, this review is designed to:

- Review status of actions to address the December 2021 review, including any changes to scope and approach, operating model, resourcing, costings, and governance.
- Assess whether the timeframe and plan for completion is achievable.
- Identify any dependencies/impacts stemming from other activities within the DTA and its Partner agencies.
- Review current funding status/future requirements.
- Identify potential risks and issues and assess plans to address these.
- Review the change management/communications plans.
- Assess whether the program is set up to ensure the realisation of benefits as defined in the business case.
- Assess the program's approach and strategies to evolve AGDIS.

The Review has six Key Focus areas:

- Achievement of Outcomes
- Stakeholders and End Users

- Governance and Planning
- Risk Management
- Review of Current Phase and Operational Effectiveness
- Readiness for Next Stage

Areas of concern/ interest of the Sponsor:

Section 1

- Canvass if governance arrangements are appropriate to sustain the Digital Identity Program for the next two years.
- How could effective communication and advertising contribute to the expansion of the AGDIS, drive public understanding and uptake as the program leverages the changes in the environment?
- Are the current governance arrangements fit for purpose and effective to ensure the successful program delivery in sustainment?
- How can the program move from the high-level benefits outlined in the business case to cost benefits analysis to demonstrate value across the broader ecosystem for instance in sustainment mode vs expanded mode?

Section 2

- Explore and provide advice for the SRO to position the Digital Identity Program to expand to whole of government.
- How could the program scale up in response to meeting demand from private sector once legislation is introduced, for instance automating the onboarding of services?
- How might the program leverage state and territories capabilities to add value to and gain commitment for expanding the AGDIS?
- What are the different capabilities including emerging technology and infrastructure, accreditation/ standards skills for example the program will need to build to ensure that it effectively meets the challenges of being a non-terminating function of government and be well positioned for the eventual expansion of the AGDIS to whole of economy?
- How would the broader governance arrangements across the ecosystem best support the AGDIS expansion.
    - Should the DTA continue with an oversight role given it would have a role to legislate, mandate rules and standards, set up a regulator and manage participants. This includes to consider if it would be appropriate for the agency leading the charge on expansion (through rules, standards etc) to oversee the implementation of myGovID and the Exchange.
    - Is there a case for these to be separately governed from the broader program? And if so, who would be best placed for this? Would Services Australia lead and govern the roll out of the exchange and myGovID?

Acknowledgements

The review team would like to thank Lucy Poole as the Senior Responsible Official and all those interviewed for their participation in the review. The support and openness from all parties contributed to the broader understanding of the program and the successful

completion of the review. Additionally, the review team would like to thank s22 and s22 for their excellent support.

Detailed Findings and Recommendations

Key Focus Areas Assessed

Achievement of Outcomes

Assessment Rating: Amber	There are issues in this Key Focus Area that require timely management attention.

Findings:

Digital Identity (DI) will make it faster and easier for people to prove who they are online and safer and easier to access government services online. DI will also increase productivity not only in the government sector, but across the nation. Since commencement in 2016, the Digital Identity Program (Program) has successfully delivered foundational DI capabilities, infrastructure and governing policy.

This assurance review is focussed on the:

- DI business case 2020/21 - funding of $256.6m over two years ending in June 2022
- MYEFO 2021 sustainability Budget – funding of $169.9 and $1.8m ending in June 2024
- s47C [redacted]

Outcomes:

Consistent with the business case, outcomes as outlined below were achieved from the $256.6m investment over the last two financial years:

s47E [redacted]

s47E [redacted]

The review team is advised that the previous government had agreed to consider a fully costed proposal in the 2022-23 Budget. To support this budget submission, the Program has undertaken a series of Inter Departmental Committee (IDC) meetings.

The three pillars that underpinned IDC discussions included:

- Improving security and trust
- Improving service delivery and inclusion
- Accelerating the Digital Economy.

Outcomes for the upcoming business case are currently being defined.

Affordability:

The current sustainability Budget provided for 2022-23 and 2023-24 through MYEFO process is inadequate to sustain DI for the medium to longer term. Currently, there is a need to provide operating Budget for the enduring (current) functions/services underpinning the DI eco- system.

The review team notes the Audit of myGov and understands that recommendations will be made to improve the usability and safety of myGov and align government initiatives. That being the case, the myGovID will need to be resourced and funded to affect these improvements and commensurate with it being entrenched as critical national infrastructure.

Benefits:

The Program has developed a benefits map and outlined benefits and their indicative measurements. The program has commenced establishing inhouse capability for benefits management and reporting. A Benefits Management Framework was developed with the aim of analysing and reporting against the committed KPIs. However, it has been paused during current phase while the Program is seeking direction from government regarding further investment and implementation of legislation.

Currently data from various sources is being gathered to set the baseline and monitor benefits against targets. The review team notes that significant work has already been undertaken in identifying data sources and learning about benefit measurements. A select set of transactional metrics has been used to measure program benefits to date. The review team recommends that priority be given to set a baseline and targets for measuring and reporting on benefits for Commonwealth agencies. In addition, processes for measuring and reporting on economy-wide benefits be solidified and implemented.

Recommendations:

Recommendation 1. Prioritise setting a baseline and targets to measure and report benefits for Commonwealth agencies and establish processes for measuring and reporting on the endorsed option which may include economy-wide benefits.

Stakeholders and End Users

Assessment Rating: Green	There are no major outstanding issues in this Key Focus Area that at this stage appear to threaten delivery significantly.

Findings:

Interviewees agreed that DI is a complex concept with many facets that present opportunities to safeguard citizens interactions with digital government services while at the same time providing convenience. While there are pockets of expertise, it is widely recognised that there is limited knowledge and expertise associated with DI in the Australian Government context. As a result, it has been difficult to message "in a simplified manner" the benefits and outcomes of DI.

Interviewees agreed that with recent data breaches by Optus and Medibank there is an opportunity to present the Program as an embedded foundational building block of safeguarding citizens and entities digital interactions with government services.

The review team notes that the program has done well in this complex environment of obtaining an understanding and alignment across a broad group of stakeholders. While there is willingness among stakeholders to find an agreed way forward, this needs to be accelerated.

The Digital Identity Program is a whole of government program led by the Digital Transformation Agency (DTA) with Services Australia, the Australian Taxation Office and Home Affairs as delivery partners. The Program is already being piloted with State and Territory jurisdictions and includes participation by private sector organisations. As such, and through providing citizens with a choice of identity providers, it is expected to facilitate whole of economy market reform for DI.

The Program has emphasised stakeholder engagement during this phase. The Program has established forums and mechanism for engagement within Commonwealth, with States/Territories and the private sector. Stakeholders include individual users, Commonwealth Government agencies, State and Territory Government agencies and private sector participants, including Australia Post and financial service providers.

All stakeholders interviewed were being actively engaged, although some would like additional clarity and regular ongoing feedback. IDCs have been held to inform planning for future phases and consult on options in the context of recent cybersecurity events such as Optus and Medibank data breaches. Stakeholders reaffirmed that a strong DI would contribute to resilience of the Australian economy and protection of citizen's personal information. It was noted that this can also improve fraud prevention as well as detection and response.

There has been strong growth in uptake of myGovID since the last review, partially driven by the COVID-19 Pandemic. This has been prompted by several developments including onboarding of Western Australian services and Director ID requirements. Stakeholders interviewed acknowledged that there were some issues experienced, e.g. notification to prepare for outages and support for large increases in users onboarding, and that some useability issues remained that need further attention. There was a desire to see usability improved and greater alignment of how DI is managed and used within the Commonwealth.

All stakeholders interviewed strongly supported the Program and the need for a DI system with interoperability. The review team noted that there were differing views among the various stakeholders about legislation and regulation, including the charging model and timing for implementation of this. Stakeholders would like certainty about arrangements through legislation and arrangements, including charging, and when this will be implemented. Program delivery partners were concerned about availability of funding after June 2024.

Stakeholders identified an opportunity for alignment on options in preparation for the next phase. In this sustainment phase the program has not been supported by a communications campaign. Stakeholders recognised the need for clear communication with the public about the implications and benefits of DI. The review team agrees with the view expressed by many stakeholders that the key message is about safety and security of Australian citizen's personal information.

Communication could include arrangements for private sector participation and choice of identity provider at an appropriate time. Stakeholders interviewed recognised an immediate need and the importance of clarifying the relationship and benefits between myGov and myGovID.

Recommendations:

Recommendation 2: On the basis that a preferred option is agreed by government, develop a communications campaign which emphasises safety and security and clarifies alignment of myGov and myGovID as part of the whole of government system.

Governance and Planning

Assessment Rating: Green	There are no major outstanding issues in this Key Focus Area that at this stage appear to threaten delivery significantly.

Findings:

Interviewees agreed that Digital Identity is a critical national digital infrastructure and a fundamental enabler of secure government service delivery and the broader digital economy. Accordingly, governance and planning need to be designed commensurate with the approved option. This may include:

- Scaling the Digital Identity Program to rapidly expand to government agencies in order to safeguard customer information and government services in the current and emerging cyber threat environment
- positioning and developing the Program to achieve the whole of economy imperatives and benefits as outlined in the approved Digital Identity business cases
- developing and sustaining a range of skills and capabilities to implement and expand Digital Identity and digital services nationally and internationally
- an effective and fit-for-purpose oversight to drive the Digital Identity policy/strategy and delivery at two levels:
    - whole of government level (WoG)
    - whole of economy level (WoE).

Governance:

The stakeholders provided positive feedback on improvements in governance and consultation over the last six months. Deputy Secretaries from four agencies have been meeting regularly to drive the Program delivery and outcomes. This successful collaboration has been key to achieving results for this complex multi-agency Program involving many internal and external stakeholders.

The Program reviewed its governance arrangements recently to provide oversight to the current sustainment phase of the Program. The governance responsibilities for the Enhanced myGov program have been transferred from the DTA to Services Australia.

Given the broad potential scope of the Program and the government's priority to safeguard customer information, moving forward beyond the sustainment phase, a fit-for-purpose governance model with clear accountabilities is required. This includes leadership and management of critical broader whole of government and whole of economy risks and an effective prioritisation process across organisations (see Section 6. Readiness for next Phase)

Planning:

Currently, the DTA, ATO and Services Australia are maintaining a Program Backlog as a repository for all work that relates to the Digital Identity Program such as new features, improvements, service requests and resolving significant bugs.

There are no plans or roadmaps beyond 30 June 2022. Moving forward with new investments, the planning processes and roadmaps for both WoE and WoG will reflect outcomes of the approved investment option, government's priorities, ambitions and risk appetite.

A Gate 5 review takes place after the entity has carried out a post-implementation review (PIR) or similar major review. It makes use of findings from that internal review, together with an assessment of organisational learning. The review team was advised that a PIR had not been completed for the Program elements completed in June 2022, however the Program has been responsive to stakeholder feedback and has incorporated improvements on an ongoing basis.

Recommendations:

Nil

Risk Management

Assessment Rating: **Amber**	There are issues in this Key Focus Area that require timely management attention.

Findings:

Risk and Issues Management Framework

The Program has a Risk Register in place (November 2022), outlining risk management activities that will be performed, recorded, and monitored. This is consistent with DTA's corporate risk management framework.

The Program has considered risks associated with evolving the Australian Digital Identity System to support whole of economy enablement of digital identity.

The review team notes that there is a high-risk profile for the Program (point in time), particularly without legislation and ongoing funding. This risk profile will change if the legislation is enacted, funding is stable, and the necessary infrastructure is established (including a Regulator) to support the enablement of Digital identity in the Australian economy.

Emerging Risks

During interviews, a wide variety of risks were raised by various interviewees, as a part of discussing the concept, structure and arrangements for the Program. Many of these risks could be classified as assumptions made with respect supporting and ensuring Program success.

These should properly be considered as risks that will have scope, time and cost implications for the Program.

A selection of areas discussed at interview include the following (non-exhaustive):

- Expansion and adoption of Digital Identity is dependent on legislation.
- Non-commonwealth agencies and the private sector cannot join the system on a permanent basis until the legislation is enacted.
- Not enacting the legislation increases the risk that jurisdictions and the private sector will begin to pursue their own initiatives that will not be interoperable with the Australian Digital Identity System, resulting in reduced convenience (value) and safety (secure) for citizens and entities.
- The Program requires ongoing (permanent) funding, including the establishment of appropriate infrastructure, resources and Government support.
- Consumer choice, whole of economy benefits and appropriate oversight will be impacted without a permanent arrangement and funding for the Regulator (accreditation function).
- Charging policies need to be agreed. That is, whether and/ or when to charge as well as who to charge. It may also require simplifying the current (proposed) charging model.
- The fragmentation of digital identity responsibilities and accountabilities within the Commonwealth, impacts the Program's ability to coordinate and deliver the proposed and future digital identity policy reforms at pace.
- s47C [redacted]

s47C [redacted]

- “Blurring” the proposed options being put forward in the 2023-24 Budget context will make it difficult for relevant Ministers to communicate and message the important benefits of digital identity.
- There are many challenges at moving at pace, of which is working in a fragmented bureaucracy along with the current skill shortage across Australia.
- The current myGov Audit presents both a risk and opportunity to the Program. Alignment with the recommendations from the myGov audit and any activities arising from this will give greater confidence for future planning.

s47C [redacted]

Thus, the assumption and risk analysis should then be incorporated into the work structure and financial model for the Program via scenario planning and sensitivity analysis.

Recommendations:

Recommendation 3: Conduct a risk management workshop, incorporating internal and external stakeholders, to inform the development of the New Policy Proposal, and incorporate emerging risks into scenario planning for each proposed option.

Review of Current Phase and Operational Effectiveness

Assessment Rating: Green	There are no major outstanding issues in this Key Focus Area that at this stage appear to threaten delivery significantly.

Findings:

The current phase has involved sustainment (holding pattern, pending a government decision of its future direction – 2023-24 Budget context) of the Digital Identity System and some enhancements with increased adoption for Commonwealth services. Pilots with jurisdictions have continued and onboarding of Western Australia led to a large increase in myGovID users. While the system is nominally in "pilot", the system is being used in earnest, supporting around 120 government services.

The Program reports that there are 126 services onboarded to use myGov with almost 10 million myGovIDs issued. Almost 7 million myGovIDs are verified and 2.8 million have facial verification. The review team was advised that up to 450,000 logons in a day occurred for the Director ID deadline which was an increase from previous highs of 300,000 for WA onboarding.

The DTA has continued to engage with stakeholders on draft legislation and arrangements for regulation, including a charging model. These arrangements are necessary for expanded participation of the private sector and to move beyond the current pilot arrangements with jurisdictions. The review team was informed that a detailed and sophisticated activity-based charging model has been developed. It is recognised by the Program that charging for accreditation under Trusted Digital Identity Framework (TDIF) is more straight-forward. Introduction of a price for transactions may be delayed until the market has matured.

An Interim Oversight Authority has been established across DTA and Services Australia. The Interim Oversight Authority monitors and manages relations with participants to operate the Digital ID system, including onboarding of reliant organisations and accreditation of organisations under TDIF. Applications for accreditation and assessment of these is continuing and can take some time.

The Interim Operating Authority produces regular reports encompassing system availability, service incidents, system change and releases and fraud and security notifications. There are appropriate artefacts and arrangements in place for management of operations, including a Security and Risk Management Plan, Business Continuity Plan and Data Sharing Framework.

The Program has reorganised to operate in sustainment mode and develop plans and options for future phases which has de-emphasised some program management activities and Program Management Office functions that were not resourced. The agency delivery partners administer their own budgets, the review team understands that funds are available for sustainment and some enhancements until June 2024.

Delivery partners are managing with the resources available for this phase and the review team were not advised of any current short-falls or resource constraints during sustainment. There had been a need to ramp up capacity as services with large numbers of users were onboarded, e.g. call centre operations. Stakeholders interviewed were concerned about certainty of funding for future sustainment and scaling of the system to onboard more services and users.

The review team was advised that during this phase the rollout of myGovID has not been supported by a communications campaign. The review team was also informed that further user research was needed to understand preferences for choice of digital ID provider. Stakeholders interviewed also raised the need to clearly communicate with the public about the implications of Digital ID, which could include private sector interoperability and charging in future.

Recommendations:

Nil

Readiness for Next Stage

Assessment Rating: **Amber**	There are issues in this Key Focus Area that require timely management attention.

Findings:

Readiness for the next stage covers the period leading up to development of the Budget submission and the Program's preparedness to implement the approved option.

In the last 12-18 months, the need for this Program has been reinforced by the ongoing pressures experienced for the access to government services online during and post COVID-19. The recent cyber related breaches in the private sector (Optus and Medibank) have further reinforced the need for this Program. Interviewees reported that these incidents have revealed more than a cyber weakness but also that proliferation of personal information and credentials across many public and private sector organisations creates vulnerabilities that are being exploited.

To continue to support the much-needed expansion of Digital Identity across the economy, the following areas of focus for the next phase of the program have been observed:

- The myGovID is viewed by stakeholders as a core asset and core infrastructure that requires continued investment as an ongoing government infrastructure program (not a project). This capability is currently in the "spot light" and is supported by good uptake. However, there is a shared view that there is a need to further embed, scale and improve the current user experience.
- s47C [redacted]
- The level of understanding of what digital identity means is limited and has complicated the journey to date. Observations suggest that there is confusion in user experience and branding between myGovID and myGov.
- There is a view that the delivery of DI should be accelerated, with robust interoperability and verifiable credentials to deal with privacy and security.
- Future cyber related breaches will inevitably occur if various organisations continue to store personal documents and IDs across the eco-system without a clear need to do so. Consideration needs to be given for the introduction of legislation to progressively prohibit the storage of individual details unless there is a legislative requirement to.
- There is a shared view that the identity space is fragmented across the Australian government. The review team is of the view that Policy and Delivery co-ordination should remain tightly coupled led by the domain experts (DTA). From a program assurance perspective, separating these capabilities may cause further fragmentation and elongate the delivery of the approved option.
- Pending government decisions, the Program will need to ramp up its delivery co-ordination capability to deliver the next phase. Governance arrangements should be reviewed again, if legislation is passed and responsibility for operation of the Digital ID system is transitioned to a regulator.
- The broad potential scope of the Program and the government's priority to safeguard customer information will require a fit-for-purpose governance model with clear accountabilities. This includes leadership and management of critical whole of

government and whole of economy risks and effective prioritisation across organisations.

Accordingly, the review team recommends based on a WoE option being approved, that the Program establishes two governing committees to drive WoE and WoG benefits:

Digital Identity WoE Governing Committee: focuses on -

- Legislation
- Regulatory body
- TDIF accreditations
- Charging framework
- Market competitiveness
- Inter-operability with accredited providers in the Digital Identity ecosystem.

Digital Identity WoG Governing Committee: focuses on delivery leadership –

- Scaling up the implementation of Digital Identity across government agencies and WoG systems (e.g. myGov)
- Making it easy for people to use digital identity
- Improving and automating onboarding process for agencies
- Building and sustaining Digital Identity capability to support government's priorities.

- Consideration needs to be given towards achieving a balanced approach for safety first versus convenience of service offerings. s47C [redacted]
- Acknowledgement needs to be given that myGov (including myGovID) is core to government's digital infrastructure. However, the introduction of interoperable and shared data credentials from state and territory offerings may enhance the Government system's ability to respond to demand. Providing choice in Identity Providers, while desirable, introduces complexity for charging and adoption. Notwithstanding policy decisions on choice of identity providers, implementation of flexibility for users can be designed as part of the system.
- s47C [redacted]
- The review team finds that there are differing views in relation to the appointment of an appropriate regulator, but the desirability of having a regulator is widely shared. Interviewees advised that appointment of a regulatory body for the Digital ID system will enable the program to increase uptake and deliver on the intended benefits. This applies for future phases seeking to extend participation by the private sector and enabling a digital market place.
- It is acknowledged that future communications need to focus on Australian citizens and be based on credentials and interactions across the government system that are safer and secure, provided government enables the usage of a digital identity as a tool. A

message articulating propriety would be beneficial e.g. “to keep you safe and keep your credentials private which enables government to deliver better services to citizens “. Consider using personas to illustrate this.

- s47C [redacted]
- The review team understands that there are several related initiatives being planned relating to biometrics and digital and data across the Commonwealth government. The review team is of the view that these measures are complementary and can be aligned to strengthen the safety and security measures for use of government services.

In readiness for future government decisions, the Program will need to considerably ramp up its program management capability to deliver on the next phase. The review team finds that Program planning and preparedness is not sufficiently developed at this stage and should be more advanced due to the complexity, high-risk profile and current uncertainty.

There are a range of program management activities that need to be established in readiness for the next phase that include resource planning, risk, issues and dependency management, and benefits monitoring. The Program needs to build and maintain increased delivery momentum.

Recommendations:

Recommendation 4: s47C [redacted] Clearly articulate the proposed options so that these are differentiated and aligned to the benefits. Include appropriate communications messaging for each option.

Recommendation 5: In anticipation of government directions and decisions on the MyGov Audit recommendations and related initiatives, be ready to “pivot”. This should include the agility and flexibility to revise options and promptly prepare for Program design, delivery and coordination.

Recommendation 6: s47C [redacted], the Program should establish two governing committees to drive the whole of government (WoG) and whole of economy (WoE) benefits.

Recommendation 7: s47C [redacted]

Appendix A: Gateway Assurance Plan

Gateway reviews complement other external and internal assurance activities and form part of the entity's overall assurance framework. Better practice indicates that developing an assurance plan for the program/project early in its life cycle is a key factor in delivering successful programs/projects. Such a plan would indicate the need for both milestone-based and time-based assurance reviews and would help ensure the program/project received the appropriate level of independent assurance.

The Gateway Assurance Plan is tabled below:

Date	Type of Review	Comments
November 2023	Mid-Stage Review	s47C [redacted]

Appendix B: Previous Recommendations

The following table outlines the recommendations made during the previous Gateway Review and the actions taken by the entity to address the recommendations.

Prior to the review, the entity should complete the 'Action Taken' column demonstrating the remedial actions taken to implement the recommendations.

The review team will review the actions taken and indicate whether the recommendations have been addressed as defined below, further comments should also be provided where recommendations have only been partially addressed or not addressed.

Fully: The recommendation has been fully implemented by the entity.

Partially: The recommendation has been partially implemented by the entity.

Not Addressed: The recommendation has not been implemented by the entity.

Previous Recommendations and Actions Taken

Item #	Recommendation	Category	Action Taken	Review Team Comments
1	Develop a benefits map for each Scenario in the McKinsey Research Report, August 2021, to guide adoption.	Essential (Do By) March 2022	The DTA has commenced establishing in-house capability for benefits management and reporting. A Benefits Realisation Framework was developed with the aim of analysing and reporting against the committed KPI's. Validation of the framework is yet to be completed. A select set of transactional metrics has been used to measure program benefits to date.	Partially Addressed. See recommendations 1 and 5 relating to differentiating benefits for each proposed option.
2	Report and track benefits accruing from Scenario 1 (in line with sustainment funding agreement).	Essential (Do By) February 2022	Digital Identity was on a trajectory of low adoption for Commonwealth use cases expected to peak at ~30%. Based on 2021 Census data Digital Identity has surpassed this target realising 44% adoption across the Australian population (15+yrs) and all identity proofing levels. Looking at identity proofing levels 2 and 3 for high-risk service, the adoption of Digital Identity sits at 31.98%.	Addressed.

Previous Recommendations and Actions Taken

3	Update the risk registers, to identify risks and their associated treatments to support transition to sustainment and ongoing operations.	Essential (Do By) February 2022	The DTA is managing its program risks on ongoing basis and maintains a current risk register in sustainment and under new governance arrangements. An internal risk management workshop was held on 1 November 2022 to update and revise the risks and mitigation strategies in place. Future risk workshops will be conducted to align emerging risks with new policy settings.	Addressed. See recommendation 3 relating to addressing emerging risk for each proposed option.
4	Evolve the assurance arrangements of the partner agencies to ensure the operational aspects of Digital Identity services are effectively assured and reported to the DTA.	Essential (Do By) June 2022	A Digital Identity Assurance plan was developed in accordance with the DTA's Assurance Framework. The Assurance Plan was endorsed by the Program Board on 17 November 2022. Change is managed in the context of the new program backlog process to drive functional enhancements.	Addressed.
5	Review and streamline the cadence of reporting to support the governance forums and to guide the program to the completion of the current tranche and to transition into sustainment.	Recommended	The DTA reviewed and streamlined its reporting to align with its new governance operating model under sustainment.	Addressed. See recommendations 6 and 7 relating to governance to support the delivery of the proposed NPP.

Previous Recommendations and Actions Taken

6	Refresh the stakeholder engagement strategy to accelerate the adoption of Digital Identity system across Commonwealth Government services to realise benefits.	Essential (Do By) Feb 2022	The DTA refreshed its stakeholder engagement strategy to June 2022. From July 2023, in line with the sustainment funding, targeted engagement for the draft charging framework and TDIF release 5 are scheduled for consultation from December 2022 through to the first quarter 2023. Ongoing consultation has been conducted with entities interested in accrediting following the EOI from 2021 and to support them their accreditation efforts. Further engagement activities with private sector including financial services, government and state and territories were held throughout the year via IDCs, working groups and one on one meetings.	Addressed.
7	Undertake a mid-stage blended Gate 5 (Tranche 1) review.	Recommended	The DTA has facilitated this mid-stagy blended Gate 5 (Tranche1) review.	Noted.

Appendix C: Review Checklist

Consistent with *Resource Management Guide 106: Australian Government Assurance Reviews*, this section contains the review team's assessment[1] of the program against each of the Key Focus Areas. Review teams apply their collective expertise to determine the relevance and appropriateness of each question below with regard to the program and review stage.

The review team provides an assessment against each of the questions to allow a level of granularity and assist entities to identify and address the key issues. The overall delivery confidence assessment for the review is provided in the Dashboard.

The review team considers the individual Key Focus Area assessment ratings below and exercises its own judgement and expertise to determine the most suitable overall assessment of delivery confidence.

Achievement of Outcomes:

Assessment Rating: Amber

	Key Focus Area Question	Comments
1.1	Strategic Fit: Is the business case up to date and does it continue to demonstrate the business need and contribute to the business strategy?	Yes.
1.2	Options: Is the preferred way forward still appropriate?	Yes, further development of the digital identity eco system is subject to a new business case
1.3	Value for Money: Are the proposed delivery arrangements likely to achieve value for money?	Yes.
1.4	Affordability: Are the costs within current budgets? Is the program/project funding affordable and supported by key stakeholders?	Partially, stakeholders emphasised the need for ongoing funding for enduring functions and further investment in expanding the digital identity capability
1.5	Achievability: Is the entity still realistic about its ability to deliver the outcomes and realise benefits?	Yes.
1.6	Organisational Change: If benefits and outcomes are dependent on organisational change, is there a plan for this, is it on track and is it achievable?	No, organisation change plans will be developed by relaying parties
1.7	Benefits: Are the outcomes delivered and the benefits to be realised understood and agreed to with benefit owners?	Yes.
1.8	Benefits: Is there a strategy and plan for realising benefits? Is it current?	Partially, further work is being undertaken. Refer to Sections 1 and 6
1.9	Has the program/project delivered the agreed outcomes? On time? On budget? Fit for purpose as approved in the business case?	Yes.

Key Focus Area Question		Comments
1.10	Are the resources necessary for operations in place?	Yes, in relation to the current sustainment phase. This will need to be ramped up pending a decision on future phases.
1.11	Where successful operations depend on organisational change, has that change been undertaken?	See 1.6 above.
1.12	Have all the governance and stakeholder issues been addressed? Including: • statutory processes • communications • external relations • environmental issues • personnel.	Yes.
1.13	Are the users satisfied with the operational service?	Yes.

Stakeholders and End Users:

Assessment Rating: Green

Key Focus Area Question		Comments
2.1	Have the stakeholders and their areas of interest been identified, and do they support the program/project?	Yes. Stakeholders include individual users, Commonwealth Government agencies, State and Territory Government agencies and private sector participants, including Australia Post, Banks and financial service providers. Stakeholders support the program and their areas of interest have been identified and considered in program planning. Individual users have adopted the solution through take-up of myGovID.
2.2	Is this a whole of government initiative or are other agencies involved in design, development or delivery?	Yes. Services Australia, the Australian Taxation Office and Home Affairs are delivery partners with the DTA.
2.3	Have stakeholder and end-user needs been taken into account in the design and delivery strategy?	Yes. Stakeholders have been extensively consulted in design and delivery of the program. The program has a stakeholder engagement strategy and supporting governance arrangements which are fit for purpose. There are stakeholder forums for Commonwealth, State and Territory governments as well as the private sector (industry based). The program has continued to consult with stakeholders and incorporate their input for development of future plans.
2.4	Do stakeholders continue to support the approved business case and the selection of the preferred option? (This includes the potential or recommended delivery approach and mechanisms.)	Yes. All stakeholders continue to support the Business Case, the need for the program, and the principle of inter-operability. There are different stakeholder views about future plans, including preferred priorities and timing.
2.5	Are the Stakeholder Engagement Strategy and supporting governance arrangements fit for purpose and do they recognise the need to engage with external whole-of-government and multi-entity stakeholders?	Yes. The Stakeholder Engagement Strategy and supporting governance arrangements are fit for purpose. There is strong and ongoing stakeholder engagement by the program. Some stakeholders reported that they would like feedback about the input they provide.
2.6	Are stakeholders confident outcomes will be achieved when expected?	Yes. Stakeholders reported that the current solution is robust and working effectively. Notwithstanding that there has been significant uptake of myGovID, interviewees acknowledged some issues with user experience and legacy system issues. As noted in 2.4, there are different views among the various stakeholders about future plans, including preferred priorities and timing. This includes possible models for regulation and charging.
2.7	Do stakeholders feel sufficiently engaged?	Yes. Stakeholder engagement has been a strength of the program. Interviewees commented that the governance arrangements are working effectively, and their input is being sought for future plans.

Governance and Planning:

Assessment Rating: Green

	Key Focus Area Question	Comments
3.1	Is there an overall program governance framework in place and is it fit for purpose? Has a steering committee, or equivalent, been established to oversee the project and is it effective?	Yes. Overall program governance structure including steering committee and program board were in place during program delivery phase which ended in June 2022. Governance suited to sustainability phase is in place.
3.2	If other agencies are involved in design and delivery , how are they included in the governance framework?	Yes.
3.3	Are program and project controls effective?	Yes.
3.4	Is there a change management process in place covering both program and organisational change requests? Is it effective?	Yes.
3.5	Are there adequate controls over scope change? Is there executive visibility? Have necessary approvals (including at government level) been secured?	Yes.
3.6	Is there a quality high level design? Does it contain sufficient detail to allow scheduling and alignment of the work to be delivered? Has it been signed off by the appropriate governance forum?	Yes. SaFe agile approach was used.
3.7	Is there executive level commitment to the program? Are responsibilities clear? Are key positions staffed?	Yes.

Risk Management:

Assessment Rating: Amber

	Key Focus Area Question	Comments
4.1	Is there an organisational framework for managing risks, assumptions , issues and dependencies (RAID) associated with this program/project?	Yes.
4.2	Have the major risks been identified and are risk owners appointed? Are the risks being effectively managed?	Yes. See Recommendation 3 associated with emerging risks.
4.3	Are there specific high level risks that might affect this program arising from, for example, multiple delivery entities, program complexity, novelty, technology, cyber issues, complex supplier arrangements or multiple stakeholders?	Yes. See Recommendation 3 associated with emerging risks.
4.4	Is the RAID log regularly reviewed and updated regularly and briefed to governance committees and management as appropriate?	Yes. November 2022.
4.5	Have assurance arrangements for the program/project been put in place and is there an Assurance Plan?	Yes. Integrity and oversight are built into the design of the system.
4.6	Are there contingency plans that address risks as necessary?	Partial. See Recommendation 3 associated with emerging risks.

Review of Current Phase and Operational Effectiveness:

Assessment Rating: Green

	Key Focus Area Question	Comments
5.1	Is there an integrated master schedule showing the program/project milestones along with the milestones and interdependencies of programs/projects (Including those managed by other agencies where relevant)?	Yes, for the June 2022 delivery. Plans were delivered in accordance with the SaFe agile approach
5.2	Milestones: Are the program/project's key milestones compliant with broader government or entity timing requirements?	Yes. The program has delivered a Digital ID and piloted this with other jurisdictions. Some private sector participants have been accredited under TDIF and others have applied. The program has also been consulting to develop options for legislation and regulation, including a model for charging.
5.3	Schedule: Are the program schedules realistic and achievable and do they include appropriate contingency?	Yes for the June 2022 delivery. Same as 5.1.
5.4	Schedule: Is the program/project progressing in accordance with the schedule?	Yes. The program has built and maintained a Digital ID system for government that supports continued uptake by citizens. There is a program back-log for future phases pending government decisions on any proposals brought forward.
5.5	Budget: Is the program/project performing to budget?	Yes. The agency delivery partners administer their own budgets, the review team understands that funds are available until June 2024.
5.6	Issues: Have issues emerged and have they been resolved?	Yes, for the June 2022 delivery. The program has reorganised to operate in sustainment mode and develop plans and options for future phases.
5.7	Does the program have a sourcing strategy? Has the program considered re-usable common design patterns either using existing technology or sourcing reusable technology?	NA. Sourcing is underway for additional Program resource but infrastructure sourcing is not required. Yes. The capability for the program has been established and is based on the ATO and Services Australia's current technology capability.
5.8	Delivery Strategy: Has a delivery strategy been developed?	Yes, for the June 2022 delivery. The program has delivered a Digital Identity System (myGovID) that links with myGov. A delivery strategy is needed for any future phase subject to government decisions.
5.9	Does the program/project have a sound Release/ Staging Strategy?	Yes. The program releases are managed appropriately using established processes.
5.10	Is functionality being released in line with that strategy?	Yes. The program has released enhancements and undertaken pilots for State and Territories.
5.11	Where relevant, has user acceptance testing and system end-to-end testing to ensure fitness for purpose been conducted and does the product/element perform to specification?	Yes. The program's delivery partners have a robust release process in place that has been adopted.

Key Focus Area Question		Comments
5.12	Outcomes and Benefits: Is the program/project and its projects on track to deliver the outcome and realise the benefits as specified in the business case?	Partial. Benefits have been identified and metrics developed. These should be tracked as part of sustainment and any future phase. Refer to Recommendation1.
5.13	Is the capability operating to defined parameters and satisfying the business need?	Partial. Operations according to agreed parameters are monitored by the Interim Oversight Authority that manages relations with participants.
5.14	Has the project documentation, training material and training program/project been delivered and kept up to date?	Yes. The Interim Oversight Authority has been established across DTA and Services Australia to manage the service.
5.15	Are the contractual relationships satisfactory?	Yes, for the current phase. The review team was advised that there are contracts in place with agencies participating in pilot arrangements and private sector organisations accredited under TDIF.
5.16	Are there plans for continued contract management?	Yes. The review team was advised that further expansion to include more private sector participants and shift beyond pilots for other jurisdictions should be supported by legislation and a regulator.
5.17	Are plans for ongoing risk management up to date?	Partial. The program reviews and updates the risk register. There are artefacts and arrangements in place for management of operations. Refer to Recommendation 3.
5.18	Are operating funds provided for smaller scale continuous improvement so the system can continue to operate as the user context changes?	Yes. Funding for sustainment and some enhancements was provided for the current phase. This funding does not continue beyond June 2024.
5.19	Have arrangements been made to report KPI for programs/projects subject to the provisions of the Digital Service Standard?	Yes. The Interim Oversight Authority has been established to monitor system performance and reports regularly on performance indicators.

Readiness for Next Stage (Guidance – this Key Focus Area is intended to cover the period leading up to the next significant milestone)

Assessment Rating: **Amber**

	Key Focus Area Question	Comments
6.1	Has the current stage successfully completed? Has approval been received from the governance committee to proceed with the next stage?	Yes, for the June 2022 delivery. Not yet. Whilst the current stage has been successfully completed and support exists in recent IDCs, s47C [redacted]
6.2	Has the entity assessed its readiness to proceed to the next stage?	Partial. Refer to Recommendation 5 and 6.
6.3	Are the funds available to undertake the next phase?	Partial. The program has been funded and operating in sustainment mode since July 2022. Terminating measure for sustainment funding ends June 2024. Funding appears not to be currently available to move the Program from 'pilot' to 'live'.
6.4	Does the program/project have the capability and capacity (right skills in the right quantity including specialist advice) to deliver the next stage?	Partial. Refer to Section 6: Readiness for Next Stage.
6.5	Are the plans for the next phase fit for purpose and achievable?	Yes. Refer to Section 6: Readiness for Next Stage.
6.6	Are the governance arrangements for the next stage fit for purpose?	Partial. Refer to Section 6: Readiness for Next Stage.
6.7	If the next gate is a Gate 5/End stage - Is there a plan for post-implementation reviews?	No. Refer to Section 3: Governance and Planning.
6.8	If the next gate is a Gate 5/End stage, is the benefits realisation plan up to date and ready to support the measurement and reporting of outcomes/benefits?	Partial. Refer to Recommendation 1 and 5.

Appendix D: List of Interviewees

s22

Name	Role/Position/Entity	Date Interviewed
[redacted]	[redacted]	[redacted]

Name	Role/Position/Entity	Date Interviewed
s22 [redacted]	[redacted]	[redacted]

Appendix E: List of Documents Reviewed

Document Title	Version no. and/or Publication date
s22 [redacted]	

Document Title	Version no. and/or Publication date
s22 [redacted]	[redacted]

Appendix F: Assessment Ratings and Definitions

Delivery Confidence Assessment Rating Definitions

The review team will provide an overall delivery confidence assessment (DCA) based on the definitions below. The review team should consider the individual Key Focus Area assessment ratings (defined below) and exercise their own judgement/expertise to determine the most suitable overall assessment of delivery confidence rating.

DCA Assessment Ratings

Assessment	Definition
Green	Successful delivery of the program to time, cost, quality standards and benefits realisation appears highly likely and there are no major outstanding issues that at this stage appear to threaten delivery significantly.
Green/Amber	Successful delivery of the program to time, cost, quality standards and benefits realisation appears probable however constant attention will be needed to ensure risks do not become major issues threatening delivery.
Amber	Successful delivery of the program to time, cost, quality standards and benefits realisation appears feasible but significant issues already exist requiring management attention. These need to be addressed promptly.
Amber/Red	Successful delivery of the program to time, cost, quality standards and benefits realisation is in doubt with major issues apparent in a number of key areas. Urgent action is needed to address these.
Red	Successful delivery of the program appears to be unachievable. There are major issues on program definition, schedule, budget, quality or benefits delivery. The program may need to be re-baselined and/or overall viability re-assessed.

Key Focus Area Assessment Rating Definitions

The review team will provide an assessment against each of the Key Focus Areas probed. This will provide a level of granularity to assist entities to identify and address the key issues.

Key Focus Area Assessment Ratings

Assessment	Definition
Green	There are no major outstanding issues in this Key Focus Area that at this stage appear to threaten delivery significantly.
Amber	There are issues in this Key Focus Area that require timely management attention.
Red	There are significant issues in this Key Focus Area that may jeopardise the successful delivery of the program.

Report Recommendation Category Definitions

The review team will rate individual recommendations with a sense of urgency as defined below:

Critical (Do Now): To increase the likelihood of a successful outcome it is of the greatest importance that the program should take action immediately.

Essential (Do By): To increase the likelihood of a successful outcome the program should take action in the near future. Whenever possible essential recommendations should be linked to program milestones (e.g. before contract signature and/or a specified timeframe i.e. within the next three months).

Recommended: The project should benefit from the uptake of this recommendation. If possible recommendations should be linked to program milestones (e.g. before contract signature and/or a specified timeframe i.e. within the next three months).