AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Applying for approval

Guidance for organisations seeking to become approved in the Australian Government Digital ID System

Version 1.4

September 2026

Acknowledgment of country

The ACCC acknowledges the traditional owners and custodians of Country throughout Australia and recognises their continuing connection to the land, sea and community. We pay our respects to them and their cultures; and to their Elders past, present and future.

Date	Version	Description
November 2024	Version 1	Initial version
February 2025	Version 1.1	Minor typographical changes
September 2025	Version 1.2	Update to Chapters 1, 2, 4, 7, 9, 10, 11 and minor administrative changes
July 2026	Version 1.3	Update to Chapters 4, 5, 7, 9 and 12 to reflect rule changes, updates to chapter numbers and minor administrative amendments
September 2026	Version 1.4	Update to section 4.2

Australian Competition and Consumer Commission
Land of the Ngunnawal people
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 09/26_26–53

www.accc.gov.au

Contents

1. Introduction

1.1 Australia's Digital ID System

Australia's Digital ID System aims to provide consumers with a secure, convenient, voluntary and inclusive way to verify their identity online.

By using a digital ID, consumers can gain greater control over their personal information and reduce the number of copies of their identity documents out in the world.

This guidance focuses on Australia's Digital ID System, which has been designed to protect consumers' privacy and security. Reflecting this, there is a robust, independent regulatory framework built into the scheme.

Australia's Digital ID System is broadly made up of 2 interconnected initiatives:

- A voluntary accreditation scheme for digital ID providers throughout the economy.
- The Australian Government Digital ID System (AGDIS).

1.2 This guidance

The purpose of this guidance is to assist organisations that are interested in applying for approval to participate in the AGDIS with lodging a valid application for approval.

The guidance also explains the legal framework governing Australia's Digital ID System, and how the Australian Competition and Consumer Commission (ACCC), in its role as the Digital ID Regulator, assesses applications for approval.

The ACCC may update this guidance periodically. Organisations should visit the Digital ID System website to ensure they are reading the latest version. The website contains detailed information for applicants and approved entities, including forms for applying for accreditation or approval to participate in the AGDIS, and an explanation of their purpose and use.

While this guidance provides general information to help organisations lodge a valid application for approval, it is not an exhaustive statement of all requirements for an application. Organisations should seek their own professional advice about the Digital ID legislation.

The ACCC's guidance does not replace the requirement for applicants and approved entities to have a full understanding of the Digital ID legislation (see section 2.1). The ACCC has prepared separate guidance to assist organisations applying for accreditation. See Applying for accreditation: Guidance for organisations seeking to become accredited in Australia's Digital ID System, available on the Digital ID System website.

Organisations should also ensure they are familiar with any guidance or other information prepared by the Office of the System Administrator (System Administrator), the Office of the Australian Information Commissioner (OAIC) and the Digital ID Data Standards Chair.

This guidance should be read in conjunction with the AGDIS System Administrator's Operational Handbook.

1.3 Participants in the AGDIS

There are separate processes for becoming accredited and approved to participate in the AGDIS. Accredited providers that wish to participate in the AGDIS are required to submit a separate application for AGDIS approval.

There are 3 types of accredited entities that can participate in the AGDIS:

- **Identity service provider** – provides services that:
  - generate, manage, maintain or verify information relating to the identity of an individual
  - generate, bind, manage or distribute authenticators to an individual
  - bind, manage or distribute authenticators generated by an individual.
- **Attribute service provider** – provides services that verify and manage an attribute of an individual.
- **Identity exchange provider** – provides services that convey, manage and coordinate the flow of information between participants in the Digital ID System.

Identity service providers, attribute service providers and identity exchange providers cannot be approved to participate in the AGDIS unless they have first been accredited.

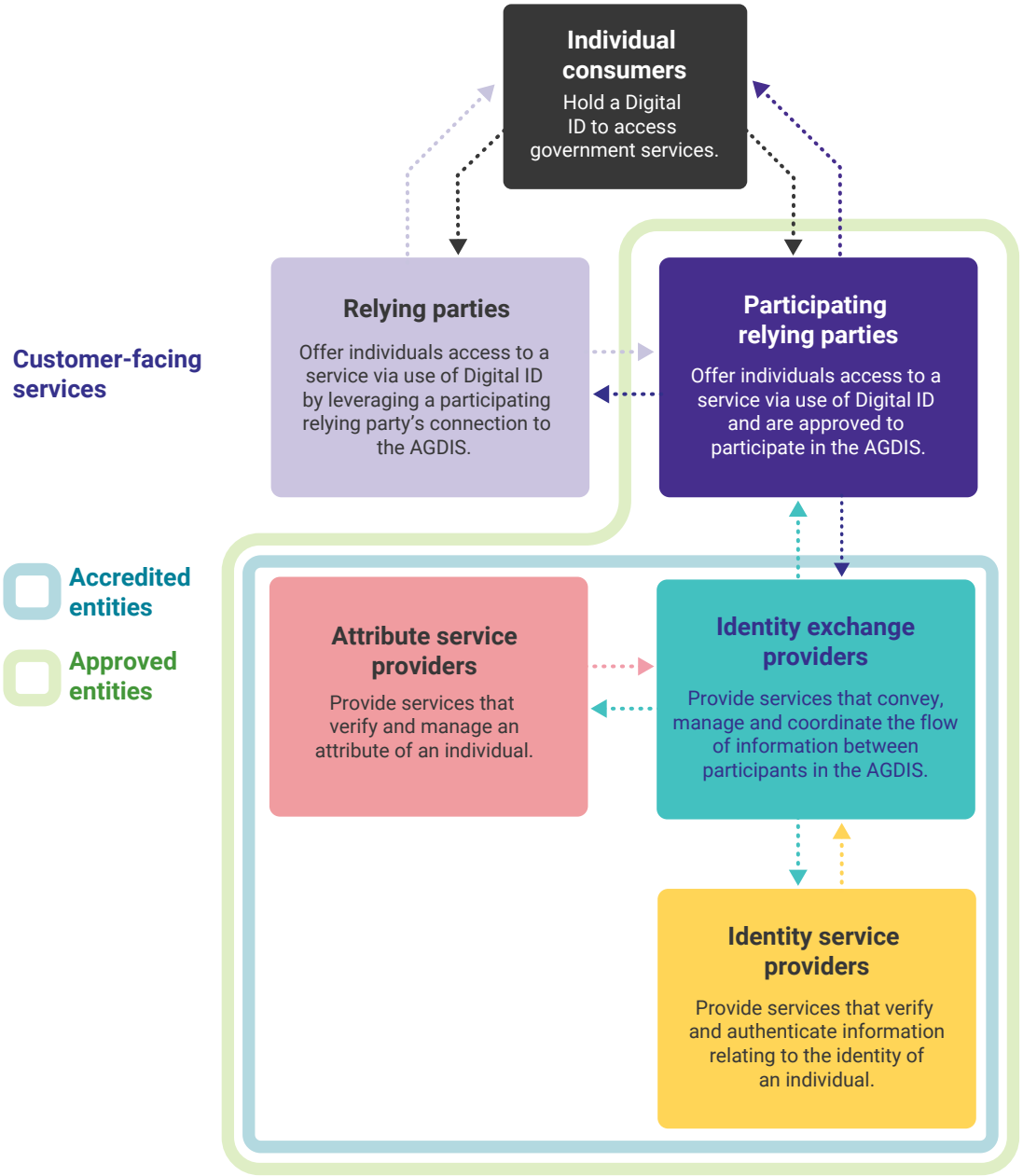
A **relying party** can also apply to participate in the AGDIS.

A relying party is an organisation that provides a service, or access to a service, to consumers by verifying the consumer's identity or attributes through an accredited entity. A relying party that wishes to participate in the AGDIS is required to apply for approval but does not need to be accredited. Once a relying party has been approved to participate in the AGDIS and its participation start date has passed, it is known as a '**participating relying party**'.

Eligibility to participate in the AGDIS is being phased. At commencement of the legislation on 30 November 2024, only government entities were eligible to participate. However, from 1 December 2026 private sector organisations can apply to participate in the AGDIS. (see section 4.1).

Figure 1 below represents the relationships between the parties in the AGDIS, where there is only a single exchange. The dotted lines represent the data flow between the parties.

Figure 1: Australian Government Digital ID System (AGDIS)



2. Regulation of Digital ID

2.1 Legal framework

The legal framework governing Australia's Digital ID system is made up of the following 3 components – the Act, the Rules and the Data Standards, collectively referred to as the Digital ID legislation.

Organisations are responsible for ensuring they familiarise themselves with and understand their obligations under the Digital ID legislation.

The Digital ID legislation (including Explanatory Statements) is available on the Federal Register of Legislation.

	Name	Explanation
Acts – The acts are supported by the below rules and data standards	*Digital ID Act 2024* (the Act)	This is the primary Act governing both the accreditation scheme and the AGDIS.
	Digital ID (Transitional and Consequential Provisions) Act 2024	This Act establishes the mechanism for how entities accredited or approved to participate in the AGDIS under the Trusted Digital Identity Framework transition into the new legislated framework.
Rules	*Digital ID Rules 2024* (the Digital ID Rules) and corresponding Explanatory Statement	These rules set out the requirements for services participating in the AGDIS, and the obligations and conditions for using the Digital ID Accreditation Trustmark.
	Digital ID (Accreditation) Rules 2024 (the Accreditation Rules) and corresponding Explanatory Statement	These rules cover the requirements entities must meet to become and remain accredited, including to manage fraud, security, privacy, accessibility, and usability, and to undertake annual reviews.
	Digital ID (Transitional and Consequential Provisions) Rules 2024 (the Transitional Rules) and corresponding Explanatory Statement	These rules provide the transitional arrangements for entities that were accredited under the Trusted Digital Identity Framework and/or participating in the unlegislated AGDIS to transition to the legislated accreditation scheme and/or to participate in the legislated AGDIS.
Standards	*Digital ID (AGDIS) Data Standards 2024* (the AGDIS Data Standards) and corresponding Explanatory Statement	These standards cover the technical integration and design requirements for entities to participate in the AGDIS.
	Digital ID (Accreditation) Data Standards 2024 (the Accreditation Data Standards) and corresponding Explanatory Statement	These standards cover the technical requirements of the accreditation scheme relating to biometric testing and the use of authentication technologies.

2.2 Agency roles

ACCC

The ACCC, in its role as the Digital ID Regulator, is responsible for promoting compliance with the Act and other legislative instruments. This includes:

- accrediting entities that provide digital ID services under the Digital ID legislation
- approving entities to participate in the AGDIS
- undertaking compliance and enforcement activities.

References to "the Regulator" throughout this guidance refer to the ACCC in its role as the Digital ID Regulator.

OAIC

The OAIC is the privacy regulator of the Digital ID System and is responsible for ensuring individuals' privacy is protected. Specifically, the OAIC's role includes:

- providing oversight of the 'additional privacy safeguards' (that apply to all accredited entities in their provision of accredited services), including developing guidance, complaint-handling, conducting investigations and taking enforcement action in respect of the additional privacy safeguards and section 136 of the Act
- performing Notifiable Data Breach scheme functions in relation to the Digital ID System
- undertaking assessments of the handling and maintenance of personal information in accordance with the Act.

The privacy obligations in the Digital ID legislation operate in addition to existing privacy obligations under either the *Privacy Act 1988* (Cth) or relevant state or territory privacy legislation.

System Administrator

The System Administrator is responsible for administering operational aspects of the AGDIS, including the integrity, and performance of the system. The System Administrator also manages applicant testing and onboards organisations that have been approved to participate in the AGDIS.

Digital ID Data Standards Chair

The Digital ID Data Standards Chair makes Digital ID Data Standards for various matters, including technical integration and design requirements for organisations to participate in the AGDIS, and other technical requirements associated with the accreditation scheme. The Data Standards Body supports the Digital ID Data Standards Chair in the delivery of its functions and powers.

The ACCC, System Administrator and the OAIC (the signatories) may, lawfully, share certain information with each other under the terms of a tripartite Memorandum of Understanding (MOU). A copy of the MOU can be found on the Digital ID System website. The MoU supports the parties to carry out their independent Digital ID functions by facilitating cooperation, consultation and legally permitted information sharing between the parties.

2.3 About the ACCC

The ACCC is an independent Commonwealth statutory authority. As well as being the Digital ID Regulator, the ACCC administers and enforces the *Competition and Consumer Act 2010* (Cth) and other legislation to promote competition and fair trading in markets for the benefit of all Australians. The ACCC also regulates national infrastructure services.

More information about the ACCC's purpose, role and structure is available at About the ACCC.

Section 90 of the Act provides that the ACCC is the Digital ID Regulator.

3. Communicating with the Regulator

All organisations that wish to make an application for AGDIS approval must first email the ACCC at DigitalIDRegulator@accc.gov.au to receive details of the submission process for completed applications.

More information about the application process is detailed throughout this guidance.

The ACCC encourages organisations to engage with the System Administrator as early as possible to conduct testing. This can occur before an application is submitted to the ACCC. Organisations should complete the registration of interest form with the System Administrator, which is available on the Digital ID System website (see section 4.3).

Approved entities that need to submit an application (for example, to add or vary a condition) should email the ACCC at DigitalIDRegulator@accc.gov.au to receive details of the submission process.

4. Before applying

4.1 Eligibility to participate in the AGDIS

Participation in the AGDIS is being rolled out in phases.

The eligibility requirements to apply to participate in the AGDIS vary depending on whether the organisation is seeking to provide accredited services or to become a participating relying party.

Organisations seeking to provide accredited services in the AGDIS must be:

- a non-corporate Commonwealth entity, or
- a state or territory government department or authority, or
- a state or territory owned corporation.

Organisations seeking to be a participating relying party in the AGDIS must be:

- a Commonwealth entity (including corporate Commonwealth entities), or
- a state or territory department or authority, or
- a state or territory owned corporation.

From 1 December 2026, private sector organisations will be able to apply to participate in the AGDIS as either participating relying parties or accredited entities.

See section 61 of the Act for the specific eligibility requirements.

The Minister for Finance has the power to manage the expansion of the AGDIS. See the Digital ID (Phasing-in of Participation in the Australian Government Digital ID System) Determination 2024 that has been made by the Minister for Finance.

4.2 Voluntariness

Voluntariness is a key principle when using a digital ID in the AGDIS. The voluntariness obligation means that when accessing services, the use of a digital ID must be voluntary.

Individuals (including those who operate businesses as sole traders) must have the option to use alternative methods to access those services, unless:

- an exception applies, or
- the Regulator has granted an exemption to the participating relying party.

This means that a participating relying party providing access to a service must generally ensure that the use of a digital ID, by individuals (including sole traders), to access that service is optional, not mandatory.

The alternative means of accessing the service:

- **must** be reasonably accessible, and
- **must not** result in the service being provided on substantially less favourable terms.

Whether the alternative means of accessing a service complies with the Act will depend on the relevant circumstances, including the type of service and the nature and characteristics of the potential users of the service. Entities are encouraged to consider vulnerable cohorts when determining the alternative means of access to their service.

Failure to comply with the voluntariness obligation may lead to enforcement action, including suspension of an approval to participate in the AGDIS.

It is recommended that participating relying parties:

- clearly and prominently state and display on their website that alternative method/s to digital ID are available to individuals (including sole traders)
- clearly communicate how to use the alternative method/s to access the service (e.g. access through email, in person, online via a secure link or username and password)
- if a service is exclusively available through an online portal, ensure access to that portal does not rely solely on a digital ID
- ensure that the alternative means is available to all individuals (including sole traders) to whom the voluntariness obligation applies.

Further guidance about the *Voluntariness Obligation in the Australian Government Digital ID System* is available on the Digital ID System website.

Exceptions to the voluntariness obligation

There are limited exceptions to the voluntariness obligation in the Act.

The exception under section 74(2) of the Act consists of 4 elements that must all be met for the exception to apply:

1. the digital ID service provides access to another service
2. the individual (including a sole trader) can access the other service by means other than the creation or use of a digital ID through the AGDIS
3. the other means is reasonably accessible, and
4. using the other means does not result in the other service being provided on substantially less favourable terms.

The exception under section 74(3)(a) of the Act is made up of 2 elements that must both be met for the exception to apply:

1. the individual (including a sole trader) accessing the service is acting on behalf of another separate legal entity, and
2. the individual is acting in a professional or business capacity.

It is important for participating relying parties to carefully assess each of the purposes for which users log into a digital platform to ensure that individuals (including sole traders) who are not acting on behalf of another entity are able to access the service through an alternative method, if an exception does not apply.

Exemption from the voluntariness obligation

The Regulator may grant an exemption from the voluntariness requirement in limited circumstances upon application by an eligible participating relying party.

The Regulator must not grant an exemption to a participating relying party that is:

- a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013* (Cth)
- a person or body that is an agency within the meaning of the *Freedom of Information Act 1982* (Cth), or
- a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982* (Cth).

Applying for a voluntariness exemption

The Regulator may grant an exemption if it is satisfied that it is appropriate to do so. Applications will be assessed by the Regulator strictly on a case-by-case basis.

An organisation can foreshadow a potential exemption request at the time of application for approval. However, an organisation can only apply for an exemption from the voluntariness obligation **after** receiving approval and has commenced participation in the AGDIS.

A mandatory consideration is that the exemption does not unduly undermine the ability of individuals to use or access a participating relying party's service.

Other factors the Regulator may consider include, but are not limited to:

- whether the applicant is a small business
- whether the applicant provides services, or access to services solely online
- whether services, or access to services are provided in exceptional circumstances
- whether the applicant has explored all other verification options
- the number and types of users impacted.

The Regulator's assessment will be guided by the requirements and objects of the Act, which include to provide individuals with secure, convenient, voluntary and inclusive ways to verify their ID in online transactions. **Given this objective, the Regulator will generally only grant exemptions to the voluntariness obligation in exceptional circumstances**.

See section 9.3 for the process for participating relying parties seeking an exemption from the voluntariness requirement.

4.3 Overview of the AGDIS application workflow

Figure 2 describes the application process and engagement across both the Regulator and the System Administrator.

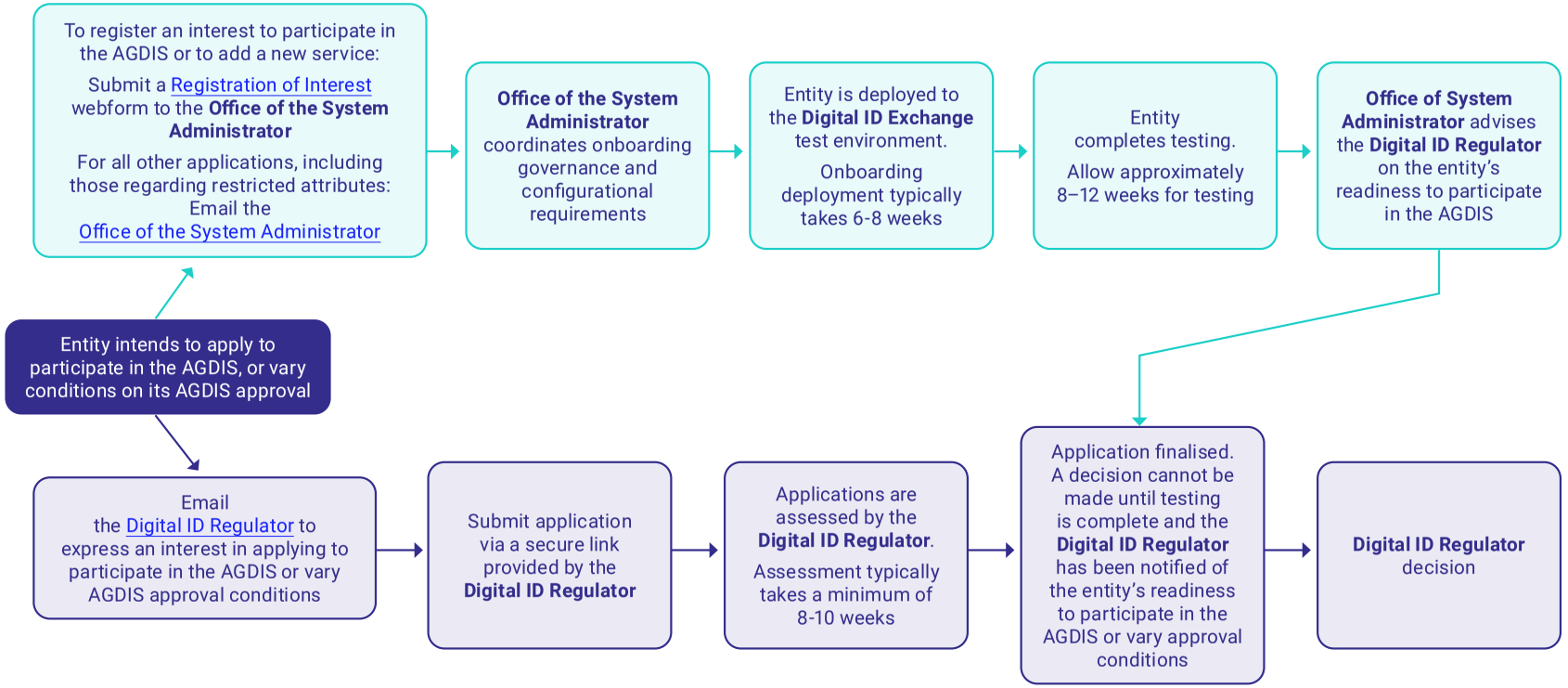
Entities are encouraged to contact the Regulator as early as possible to support a smooth application process and ensure timely progress.

Figure 2: Engagement with the Regulator and the System Administrator

AUSTRALIAN COMPETITION & CONSUMER COMMISSION

The Australian Government Digital ID System (AGDIS) application workflow

This workflow provides a high-level overview in relation to AGDIS applications (including applying to participate in the AGDIS or varying conditions). Entities will need to engage with both the Digital ID Regulator and the Office of the System Administrator.



See figure 3 for details on the Regulator application process.

4.4 Testing with the System Administrator

All organisations that wish to apply to participate in the AGDIS must complete a registration of interest form with the System Administrator. The *AGDIS System Administrator registration of interest form* is available on the Digital ID System website.

The System Administrator facilitates onboarding to the AGDIS test environment following receipt of a registration of interest. Organisations can start testing before or after applying to the Regulator for approval to participate in the AGDIS; however, approval to participate will not be granted until testing is completed. Successful completion of testing does not mean an application for approval will be granted.

5. Regulator's assessment

5.1 Prioritisation of applications

The Regulator will prioritise applications based on the date of receipt of a complete application.

There are some exceptions for urgent applications, which may require a triage approach. These exceptions could include a request to vary a participation start date, or to suspend or revoke an approval; however, in general, all applications are processed in the order in which a complete application is received. This ensures a fair process. The Regulator will not start progressing an application if it is incomplete.

5.2 Timeframes for application assessment

The Regulator will assess an application as promptly as possible. The timeframe may vary depending on the complexity of the application, the completeness of the documentation provided and the volume of other applications under review. As a general estimate, the assessment process of a complete application typically takes a minimum **8–10 weeks**. Entities with fixed timeframes or commitments should allocate sufficient time for the assessment process. They are also encouraged to contact the Regulator if they have any concerns about their application prior to submission.

5.3 Completeness check

For the Regulator to assess an application to participate in the AGDIS, the applicant must have submitted a completed *Application to participate in the AGDIS form* (see section 7.2), and associated documents. If the Regulator identifies any gaps or deficiencies during the completeness check, it will advise the applicant of the issues requiring rectification prior to re-submission. Incomplete applications requiring follow up will take longer to process, as the assessment only proceeds once the application is complete and can be prioritised accordingly.

5.4 Assessment

If an application is complete, it will proceed to the assessment stage.

To approve an application to participate in the AGDIS, the Regulator must be satisfied that:

- the applicant has completed testing
- the applicant will comply with the relevant Digital ID Data Standards that apply both to the applicant and to participation in the AGDIS
- the applicant will comply with the Act and any requirements of the Digital ID Rules and Accreditation Rules if, applicable
- the applicant has effective plans and procedures as required by the Digital ID Rules
- it is appropriate to approve the applicant, which may include whether the applicant is a fit and proper person.

In undertaking its assessment, the Regulator may request further information or documentation if required.

The Regulator may also:

- engage with the applicant to seek clarification or ask for further information on an application
- consult or share information with other Australian Government authorities such as the OAIC, national security agencies, or similar authorities overseas
- consult with independent assessors on whether the applicant will be able to comply with the relevant legislative requirements.

5.5 Decision

The Regulator will notify the applicant in writing about its decision to grant or refuse approval to participate in the AGDIS.

If the Regulator decides to not grant approval, it will provide reasons for the decision and information about the applicant's rights to have the decision reviewed (see section 10 for further information about reviewable decisions).

6. Conditions on AGDIS approval

If granted approval, entities must comply with the relevant conditions on their approval. Failure to do so may result in suspension or revocation of an entity's approval.

Some conditions are imposed by default by the Act and the Digital ID Rules. For example, a default condition that applies broadly is simply that approved entities must comply with the Act (see section 64 of the Act).

For accredited entities, conditions applied to their accreditation will be automatically applied to any AGDIS approval, should it be granted. Additional conditions may be applied to AGDIS approvals. Conditions applying to an accredited entity's approval cannot be more permissive than the conditions the entity holds as an accredited service provider.

6.1 Conditions requested by an applicant

Applicants may apply for conditions to be imposed during the approval application process (see section 8.1). If approval is granted, entities may also apply for conditions to be imposed, varied or revoked. See *Guidance for entities approved to participate in the Australian Government Digital System* available on the Digital ID System website for information about the application process for a condition to be imposed, varied or revoked.

Applicants should review the default conditions under the Act, Accreditation Rules, and Digital ID Rules before applying to the Regulator for a condition to be imposed.

Applicants applying for conditions to be imposed are required to provide details, justification and supporting evidence relevant to the condition(s) they are seeking. Supporting evidence might include plans and procedures for how an applicant will comply with the condition.

See sections 16–19 of the Act, Part 7.2 of the Accreditation Rules, and Chapter 3 Part 2 of the Digital ID Rules for information about conditions.

6.2 Conditions imposed by the Regulator or Minister

The Regulator may impose conditions to define the scope of approved services the entity can provide or provide access to.

Additional conditions can also be imposed by the Regulator at any time if it considers it appropriate in the circumstances, such as:

- whether the entity is authorised to collect or disclose a restricted attribute and/or biometric information
- to direct entities to engage in certain conduct or take certain action, including:
  - directing an entity to take certain actions before suspending or revoking its approval
  - directing an entity to maintain adequate insurance against any liabilities arising in connection with the obligations under the statutory contract between entities participating in the AGDIS.

The Regulator must impose conditions if directed to do so by the Minister for Finance for reasons of national security.

6.3 Services

The services an entity is approved to provide, or provide access to, will be listed as a condition of its approval. If an entity wishes to add, vary or no longer offer (revoke) a service, it will need to submit an application to impose, vary or revoke a condition. See *Guidance for entities approved to participate in the Australian Government Digital System* available on the Digital ID System website for information about the application process for a condition to be imposed, varied or revoked.

7. AGDIS application steps

7.1 Registration

As part of making an application, an organisation should submit the following forms, available on the Digital ID system website:

- *Organisation and Authorised Officer form* – used by an organisation to provide the Regulator with information about:
  - the organisation that is applying to be approved
  - the Authorised Officer, which is a person who is authorised to act on behalf of the organisation
  - the primary contact person/s for the organisation.
- *Service and Contact Person form* – used by an organisation to provide the Regulator with information about:
  - a service seeking approval, to participate in the AGDIS under the Act
  - seeking approval, or already approved, to participate in the AGDIS
  - the contact person/s for the service.

7.2 AGDIS application form

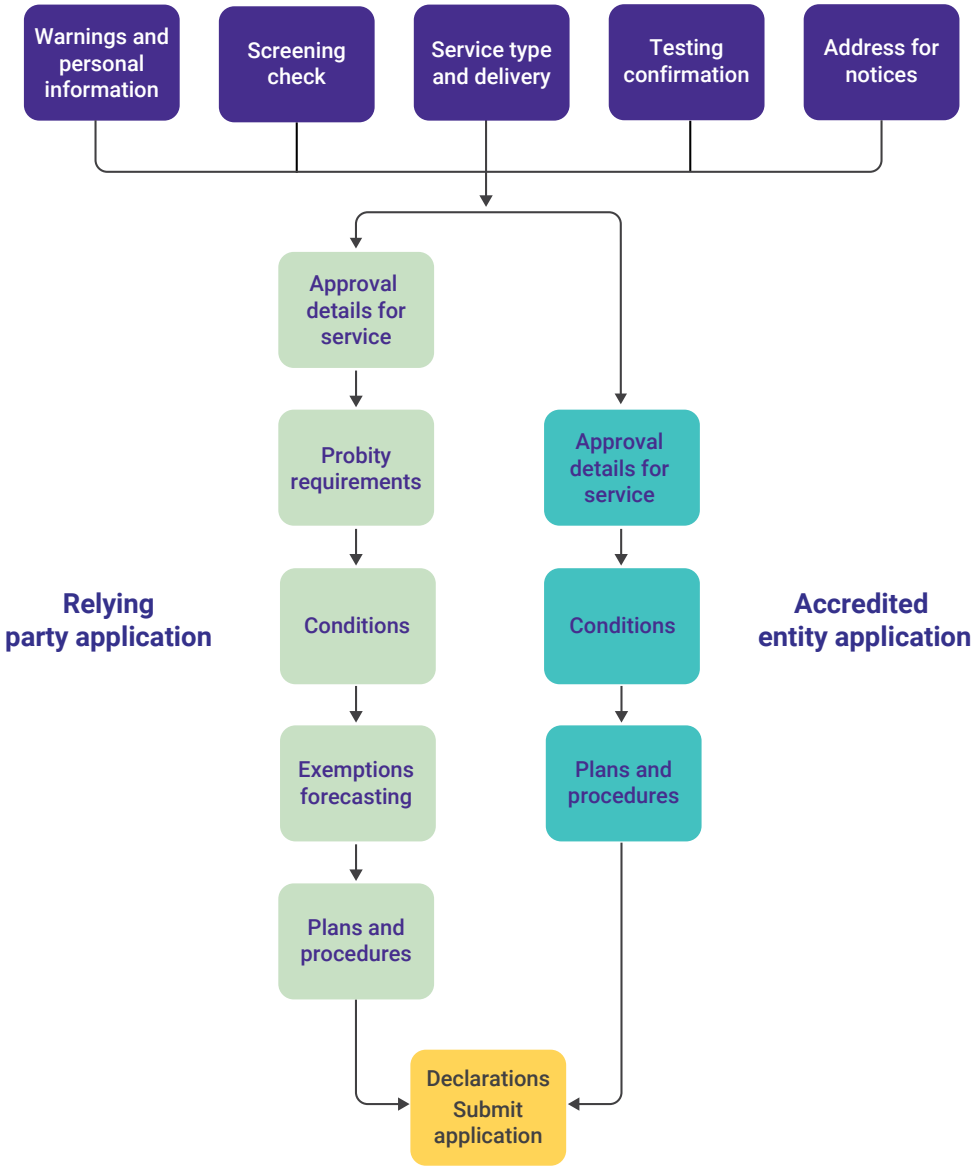
An organisation seeking to become approved to participate in the AGDIS is required to use the Regulator's *Application to participate in the AGDIS form* (application form). This form is available on the Digital ID System website and must be submitted to the Regulator. All applicants should familiarise themselves with this form to support them in preparing the required application.

Where an organisation is applying to become approved to participate in the AGDIS for the first time, a separate application form will be required for each service requested. If approval is granted and the organisation wishes to add additional services, they must request this via the *Conditions on Accreditation and AGDIS Approvals form* (see *Guidance for entities approved to participate in the Australian Government Digital System* available on the Digital ID System website).

Completing an application

The Regulator application process is represented in Figure 3. For the Regulator to assess an application to participate in the AGDIS, the applicant must have submitted the completed application form with all required documents.

Figure 3: AGDIS – The Regulator application process



7.3 Screening check

All organisations applying for approval to participate in the AGDIS must complete a screening check as part of the application form.

The screening check is to ensure applicants have all required information and documents before applying. It is also designed to ensure applicants understand and agree to critical requirements before commencing their application, including:

- eligibility requirements
- the requirement to comply with all Digital ID legislation, including the Act, Digital ID Rules, Accreditation Rules, Digital ID Data Standards and the services for which they are seeking approval
- the requirement to commence participating in the AGDIS on the specified participation start date (see section 11.1)
- having in place all plans and written procedures for required matters.

7.4 Approval type and details

After the screening check, all applicants will need to select the service and the type of approval they are applying for. The participating entity types are:

- Accredited entity (see section 8)
  - attribute service provider
  - identity exchange provider
  - identity service provider.
- Participating relying party (see section 9).

Applicants can only add one service per application. However, applicants can submit separate applications if they are seeking approval to provide multiple services or become multiple provider types.

Service connections

Participating relying parties can offer services which connect directly to the AGDIS or via an indirect connection.

Participating relying parties must apply for all services they provide, or provide access to, to be approved as a condition on their approval, regardless of whether the service connects directly to the AGDIS or via an indirect connection.

The indirect connection enables multiple services to access the AGDIS using a single connection rather than requiring each service to connect directly to the AGDIS, regardless of who owns the service. The indirect connection means relying parties can leverage their relationships with participating relying parties to verify individuals' attributes and digital ID in the AGDIS, rather than seeking approval to participate individually.

Entities offering services which access the AGDIS via an indirect connection can apply to collect or disclose restricted attributes. However, the Regulator encourages entities which may seek to collect or disclose restricted attributes to access the AGDIS via a direct connection (rather than an indirect connection).

To support visibility of these arrangements, applicants will be required to confirm:

- what service they are seeking to have approved
- who owns the service
- whether other organisations are responsible for the delivery of the service and, if so, who they are and what roles they hold
- whether the service they are applying for will access the AGDIS directly or via an indirect connection. If an applicant intends for its service to access the AGDIS via an indirect connection, it will be required to detail which service it intends to use to connect to the AGDIS.

It is important for applicants to understand that, if approved to participate in the AGDIS, they are responsible for providing contact information and responding to any events notified to them by the Regulator or the System Administrator regarding the provision of the service for which they are approved. This includes where the service has multiple organisations responsible for its delivery.

Applicants are also responsible for any compliance issues arising in relation to the approved service, even where the service has multiple organisations responsible for its delivery.

7.5 Application form

The *Application to participate in the AGDIS form* has 2 separate work streams:

- Applying to participate as an accredited entity (see section 8).
- Applying to participate as a participating relying party (see section 9).

7.6 Declarations

Prior to finalising an application, all applicants will be required to:

- confirm they understand their legal obligations under the Act, Rules, and Data Standards, via the signed declaration form: *Declaration for compliance for all entities applying to participate in the AGDIS*, available on the Digital ID System website
- confirm that all information provided as part of the application is true and complete via the signed declaration form: *Final Declaration for all entities seeking approval to participate in the AGDIS*, available on the Digital ID System website.

Participating relying parties will also be required to declare their organisation has in place the required written procedures to notify the System Administrator, written cyber security plan, digital ID fraud management plan and written disaster recovery and business continuity plan via the signed declaration form: *Plans and procedure declarations for relying parties applying to participate in the AGDIS*, available on the Digital ID System website.

Accredited entities will also be required to declare their organisation has in place the required written procedures to notify the System Administrator via the signed declaration form: *Plans and procedures declaration for accredited entities seeking approval to participate in the AGDIS*, available on the Digital ID System website.

From 1 July 2026, identity service providers and attribute service providers may be required to declare that their organisation has in place published policies related to:

- the identification, management and resolution of cyber security incidents and digital ID fraud incidents that occur, or are reasonably suspected of having occurred, in relation to their accredited services in the AGDIS
- complaints by individuals relating to cyber security incidents and digital ID fraud incidents that occur, or are reasonably suspected of having occurred, in relation to their accredited services in the AGDIS. Further specifications of these requirements can be found in Part 5 of Chapter 4A of the *Digital ID Rules*.

7.7 Machinery of Government change

To minimise disruption to services within the AGDIS and reduce administrative and regulatory burden, the Digital ID Rules establish a streamlined application process to assist participating relying parties affected by a Machinery of Government (MoG) change. See section 9.5 for more detail.

8. Applying to participate as an accredited entity

8.1 Applying for conditions

As outlined in section 6, conditions already applied to an accredited entity will be automatically applied to any AGDIS approval, should it be granted. Applicants can request additional conditions to be applied to their approval to participate in the AGDIS. However, these conditions must not be more permissive than the conditions applying to their accreditation.

Should an accredited entity wish to request approval conditions that are more permissive than conditions originally granted for its accreditation, it must first apply to vary its accreditation conditions (see the Regulator's *Guidance for accredited entities in Australia's Digital ID System*, available on the Digital ID System website). For example, accredited entities cannot offer services in the AGDIS which are not captured in their accreditation conditions as that type of provider. This rule does not apply if an accredited entity is applying to participate in the AGDIS as a participating relying party.

If the application to vary accreditation conditions is granted, it will be applied to the accredited entity's AGDIS approval.

Where an accredited entity seeks to apply conditions specifically to its AGDIS approval, the following details will be required:

- the condition being sought
- justification for the condition to be imposed
- whether the condition should have a specific start and end date
- any relevant supporting evidence.

8.2 Plans and procedures

Accredited entities must declare they have written procedures for notifying the System Administrator in the event:

- their IT system that interacts with the AGDIS changes in a material way
- an IT system outage (planned or unplanned) occurs that could have a material effect on the operation of the AGDIS.

The Regulator may request further information and documents as part of its assessment of this requirement.

See Rule 3.2 of the Digital ID Rules for the requirements relating to notifying the System Administrator.

8.3 AGDIS Redress framework

Rule 7.1(4) of the *Digital ID Rules* sets out that, in relation to the AGDIS Redress framework, from 1 July 2026, identity service providers and attribute service providers (that have not had their approval to participate suspended or revoked) must develop and publish specific policies relating to incidents and complaints from 1 July 2026.

See Parts 4 and 5 of Chapter 4A the Digital ID Rules for requirements around support for individuals, and policies related to incidents and complaints.

See section 12.3 for more detail on the AGDIS Redress framework requirements. See also *Guidance for entities approved to participate in the AGDIS* available on the Digital ID System website.

See section Chapter 4A of the Rules for details on the AGDIS Redress framework.

9. Applying as a participating relying party

9.1 Appropriateness to participate in the AGDIS

Before approving an application to participate in the AGDIS, the Regulator must be satisfied it is appropriate to approve the applicant in light of the objects of the Act, which include promoting privacy, the security of personal information, and trust in digital ID services amongst the Australian community.

In deciding whether it is appropriate to approve an applicant to participate in the AGDIS, the Regulator may have regard to whether the organisation is a fit and proper person and any other matters the Regulator considers relevant.

To assist this determination, applicants for approval must complete the E*vidence it is appropriate to accredit or approve the organisation form* (evidence of appropriateness form) and submit the form and associated documents with the application. The evidence of appropriateness form is available on the Digital ID System website.

The evidence of appropriateness form allows an organisation to demonstrate it is appropriate for the Regulator to approve them, by electing to either:

- provide evidence in line with the fit and proper person test as set out in Chapter 2 of the Digital ID Rules, or
- provide alternative evidence to satisfy the Regulator.

Receiving entities that are subject to the streamlined application process (see section 9.5 for more information on Machinery of Government changes) established under the Rules are still required to complete the evidence of appropriateness form and submit associated documents as part of their application.

Further information on these options is set out in the sections below.

Fit and proper person test or alternative evidence

When deciding whether to approve an applicant, the Regulator may have regard to whether the applicant is a 'fit and proper person'. If the Regulator does consider whether an applicant is a fit and proper person, it must consider the fit and proper person test set out in the Digital ID Rules, which set out a number of mandatory matters (including but not limited to whether the applicant has been convicted of a serious criminal offence or has a history of insolvency or bankruptcy). The Regulator is not, however, required to consider these mandatory matters when considering a streamlined application from a receiving entity (see section 9.5).

Due to the broad range of organisations that may seek approval, including government organisations and private entities, the criteria in the fit and proper person test may not be relevant to all applicants. For some applicants, there may be alternative evidence that is more pertinent to determining if it is appropriate to approve the organisation to participate in the AGDIS. For this reason, the Regulator has discretion about whether it is necessary to consider the fit and proper person test for all applications.

Whether an applicant will be able to satisfy the Regulator it is appropriate to approve the organisation without providing evidence in line with the fit and proper person test set out in the Digital ID Rules will depend on the circumstances.

The Regulator expects most applicants to provide evidence in line with the fit and proper person test. However, examples of circumstances where it may be appropriate for an applicant to provide alternative evidence to satisfy the Regulator include:

- The organisation has **previously been accredited or approved to participate in the AGDIS** under the Act – for example, if an organisation accredited as an identity service provider later seeks to also be accredited as an attribute service provider.
- In this scenario, the Regulator would have already assessed the appropriateness of the organisation to be accredited, and the organisation will be subject to ongoing reporting obligations in relation to their fitness and propriety.
- The organisation is currently **accredited under the Consumer Data Right regime**.
- The fit and proper person test under the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) and the fit and proper person test in the Digital ID Rules are substantially similar. Organisations accredited under the Consumer Data Right regime also have ongoing reporting obligations in relation to fitness and propriety.
- The organisation is a **non-corporate Commonwealth entity** such as a department of state, a parliamentary department, or an entity prescribed by legislation.
- These entities are subject to a high level of oversight and accountability obligations, and their officials are subject to ongoing statutory duties which relate to fitness and propriety, such as under the *Public Governance, Performance and Accountability Act 2013* (Cth). Alternative evidence of the organisation's oversight and accountability frameworks, and compliance with their ongoing statutory duties, may be more pertinent to the Regulator's assessment of appropriateness than some of the mandatory matters set out in the Digital ID Rules.
- The organisation is **subject to other significant regulatory controls** relating to oversight and accountability, character obligations of employees, and privacy obligations, or is **subject to other similar fit and proper person tests**.

An organisation that falls within one or more of the above categories may still prefer to provide evidence in line with the fit and proper person test set out in the Digital ID Rules.

Whatever evidence the applicant provides, the Regulator will request further information and documents if required to be satisfied it is appropriate to approve the applicant, in line with the objects of the Act.

If an applicant chooses to provide alternative evidence, the Regulator may request it provide evidence in line with the fit and proper person test in the Digital ID Rules if the Regulator is not satisfied it is appropriate to approve the applicant on the basis of the alternative evidence provided. This may extend the timeframes for assessment of the application for approval.

Evidence in line with the fit and proper person test

The information in this section is relevant to an applicant that has elected to provide evidence in line with the fit and proper person test set out in the Digital ID Rules.

Documents to be submitted with the application

- ☐ *Completed Evidence it is appropriate to accredit or approve the organisation form.*
- ☐ *Current organisation chart reflecting all relevant associated persons and their relationships with the organisation.*
- ☐ *If the organisation is a body corporate – current corporate structure chart that identifies the organisation and its associates and associated entities (within the meaning of the Corporations Act 2001 (Cth)).*
- ☐ *Associated persons declarations via the Fit and proper declaration for associated persons form – the organisation must provide a separate signed declaration from each associated person. The template declaration form is available on the Digital ID System website.*

To the extent any of this information has been provided in response to other sections of the approval application form there is no need to provide the information again – instead an organisation can refer to the relevant document or response.

The Regulator will consider whether the organisation, and associated person/s (see section on associated persons below) of the organisation, has:

- within the previous 10 years, been convicted or found guilty of a serious criminal offence or an offence of dishonesty against any law of the Commonwealth or of a State or Territory, or a law of a foreign jurisdiction
- been found to have contravened a law relevant to the management of its DI data environment or a similar law of a foreign jurisdiction. Which laws are relevant will depend on the organisation's circumstances, including the type of organisation, the industry it operates in and the data it proposes to handle. Laws likely to be relevant include, but are not limited to:
  - the Act, Accreditation Rules and Digital ID Rules
  - *Privacy Act 1988* (Cth) and similar State or Territory laws
  - *Corporations Act 2001* (Cth)
  - *Corporations Regulations 2001* (Cth)
  - *Security of Critical Infrastructure Act 2018* (Cth)
- been the subject of a determination under sections 52(1)(b) or 52(1A) (a)–(d) of the *Privacy Act 1988* (Cth), which relates to an interference with the privacy of an individual, or a finding or determination of a similar nature under a similar law of a State or Territory or a foreign jurisdiction
- a history of insolvency or bankruptcy, and/or
- been the subject of a determination made under an external dispute resolution scheme that included a requirement to pay compensation and was, at the time the determination was made, recognised under section 35A of the *Privacy Act 1988* (Cth) or section 56DA of the *Competition and Consumer Act 2010* (Cth) (which sets out recognised external dispute resolution schemes for the purposes of the Consumer Data Right).

If the organisation is a body corporate, the Regulator will also consider whether any of the directors of the organisation, or of an associated person of the organisation, have been disqualified from managing corporations or been subject to a banning order.

The Regulator will also have regard to whether the organisation has previously had an application to be accredited or approved to participate in the AGDIS refused. If the organisation is or has been accredited or approved, the Regulator will consider whether that accreditation or approval has been suspended or revoked.

An organisation should disclose any other matters that may negatively impact the Regulator's assessment of whether the organisation is a fit and proper person. This could include details of any:

- investigation or disciplinary action by a professional body
- inquiry or investigation by a government agency
- court proceedings initiated by a government agency
- data breaches that have impacted the organisation and the organisation's response.

The Regulator may conduct searches and undertake relevant checks to verify the information and documents provided by the organisation. This may include criminal background checks of associated persons.

Associated persons

An applicant providing evidence in line with the fit and proper person test is required to provide the names of all associated persons and their relationship to the organisation as part of the evidence of appropriateness form. An applicant must also provide a separate signed declaration from each associated person addressing the criteria in the fit and proper person test: *Fit and Proper Person Declaration for Associated Persons form*. The template declaration form is available on the Digital ID System website.

Identifying associated persons

'Associated person' is defined in rule 1.4 of the Digital ID Rules. It is essential that an organisation carefully considers the definition of 'associated person' and identifies all their associated persons, even if there is a substantial number of them.

When determining who their associated persons are, an organisation should:

- consider which persons – within or outside their organisation – make, or participate in making, decisions that affect the performance of the organisation's functions when operating in the AGDIS, or have the capacity to significantly affect the performance of the organisation's functions when operating in the AGDIS. This may include:
  - office holders, for instance a director or company secretary
  - operations managers or data security managers
  - accountable executives, for instance a senior executive of the organisation responsible for the overall management of the organisation's functions when operating in the AGDIS
  - any other staff who have influence over the work that could significantly affect or influence the performance of the organisation's functions when operating in the AGDIS
  - any relevant contractors
- if the organisation is a body corporate – also refer to the definitions of associate and associated entity in the *Corporations Act 2001* (Cth). These definitions encompass a wide group of individual

and corporate persons associated with the organisation, including persons who belong to overseas entities. For example, an associated entity can include related bodies corporate such as a holding company or a subsidiary, and an associate can include a director or company secretary of either of those entities.

An organisation may wish to seek appropriate professional advice to assist with identifying their associated persons.

Alternative evidence of appropriateness

The information in this section is relevant to an applicant that has elected to provide alternative evidence to satisfy the Regulator it is appropriate to approve them.

Documents to be submitted with the application

- ☐ *Completed Evidence it is appropriate to accredit or approve the organisation form.*
- ☐ *Any documents that detail or support the information provided in the evidence of appropriateness form.*
- ☐ *If the organisation is a body corporate – current corporate structure chart that identifies the organisation, its subsidiaries, and its related bodies corporate.*
- ☐ *Current organisation chart identifying any persons who have the capacity to significantly affect the performance of the organisation's functions when operating in the AGDIS.*

To the extent any of this information has been provided in response to other sections of the approval application form there is no need to provide the information again – instead an organisation can refer to the relevant document or response.

The Regulator will consider whether the organisation, and any persons that have the capacity to significantly affect the performance of the organisation's functions when operating in the AGDIS, possess appropriate qualities such as *competence, character, diligence, honesty, integrity, and judgement*. The Regulator will also consider whether the organisation has sufficient processes or controls in place to ensure the organisation and its key relevant persons maintain and act in accordance with these qualities.

Types of alternative evidence

The types of evidence an applicant should provide, as well as the level of detail required, will depend on its individual circumstances.

Information likely to be relevant includes:

- Details of any **relevant legislative or regulatory controls** that apply to the organisation or its employees, particularly controls relating to oversight and accountability, character obligations of employees, and privacy obligations. For example, authorised deposit-taking institutions are regulated by the Australian Prudential Regulation Authority, Commonwealth companies and entities are subject to the *Public Governance, Performance and Accountability Act 2013* (Cth) and Australian Public Service employees are subject to the *Public Service Act 1999* (Cth).
- Details of any **similar fit and proper person tests** under other regulatory regimes the organisation or its employees have been subject to, e.g. most entities accredited under the Consumer Data Right regime will have been subject to a similar fit and proper person test during that accreditation

process. The more similar the other fit and proper person test is to the mandatory matters set out in the Digital ID Rules, the more likely it is to be relevant.

Details of **pre-employment checks** the organisation conducts, e.g. whether relevant staff and/or directors are subject to police and/or security checks.

For government organisations, relevant information may also include:

- details of the organisation's status, e.g. whether the organisation is a central government agency or department, or, if the organisation is a corporation, who controls it
- whether there is an accountable authority responsible for the organisation and, if so, what the obligations of this authority are
- whether the organisation is generally subject to government policy and directions
- whether the organisation is subject to Ministerial or other governmental control over its operations
- whether the organisation is subject to reporting obligations to the relevant government
- whether the organisation is subject to auditing obligations to the relevant government
- whether the organisation is otherwise subject to oversight over its operations
- whether the organisation is subject to public interest disclosure obligations.

Adverse information

An applicant should also disclose any other matters that may negatively impact the Regulator's assessment of whether it is appropriate to approve it. This could include details of any:

- investigation or disciplinary action by a professional body
- inquiry or investigation by a government agency
- court proceedings initiated by a government agency
- details of any data breaches that have impacted the organisation and the organisation's response.

The Regulator may conduct searches and undertake relevant checks to verify the information and documents provided by the applicant. This may include criminal background checks.

Ongoing reporting requirements

Approved entities are required to notify the Regulator within 5 business days of any matter that could be relevant to a decision as to whether they are a fit and proper person. Importantly, this reporting obligation applies even if the entity does not provide evidence in line with the fit and proper person test as part of its application for approval.

The Regulator may suspend or revoke an entity's approval if it is satisfied that it is not appropriate for the entity to be approved. In deciding this, the Regulator may have regard to the fit and proper person test.

Voluntariness obligation

The Regulator will assess whether the entity complies with the voluntariness obligation (see section 4.2) and may request supporting evidence in relation to this. Entities should ensure that the alternative access methods they provide is reasonably accessible to disadvantaged, or vulnerable user groups.

9.2 Applying for conditions

Participating relying party applicants may apply for conditions to be imposed at either the organisation level or the service level.

Where a participating relying party applicant seeks to apply for conditions, the following details will be required:

- the condition being sought
- justification for the condition to be imposed
- whether the condition should have a specific start and end date
- any relevant supporting evidence.

Restricted attribute collection

The Act includes strong safeguards regarding restricted attributes of individuals.

Participating relying parties can only collect and disclose restricted attributes if they are necessary for the service that a customer is accessing, and a condition of their approval authorises them to do so. Examples of restricted attributes include health information, information about a criminal record, or an identifier of an individual contained on a government issued document.

See section 11 of the Act for the meaning, as well as examples, of restricted attribute of an individual.

If an organisation applies for a condition to collect or disclose restricted attributes of individuals, the application form should include detailed information and relevant documents in response to all relevant questions, including:

- details of proposed arrangements to mitigate the risks of cyber security and fraud incidents when collecting or disclosing restricted attributes
- controls aligning with requirements in relation to the collection or disclosure of restricted attributes
- the restricted attributes sought to be collected or disclosed and reasons for the need to collect or disclose these attributes
- identifying potential harm of disclosure and community expectations around handling this information.

The Regulator will have regard to all the information provided, relevant legislative requirements and any other matters it considers relevant when deciding whether it is appropriate in the circumstances to impose the condition.

The Regulator will consider all applications for a condition to collect or disclose restricted attributes in line with the relevant provisions in the Digital ID legislation. Although not an express legislative requirement, a direct connection to the AGDIS is encouraged to mitigate the risks of cyber security and fraud incidents when collecting or disclosing restricted attributes.

9.3 Exemptions forecasting (voluntariness)

Applicants are not eligible to apply for voluntariness exemption until they become a participating relying party (i.e. after they are participating in the AGDIS). However, the *Application to participate in the AGDIS form* seeks preliminary information as to whether a participating relying party applicant intends to seek an exemption from the voluntariness obligation for a service.

If the applicant is approved to become a participating relying party, it will then need to apply separately for exemption from the voluntariness obligation. The Regulator may grant this in exceptional circumstances and where it is satisfied it is appropriate to do so (see section 4.2).

The application for exemption is to be made via the *AGDIS exemptions for participating relying parties form*, available on the Digital ID System website, and submitted to the Regulator.

The application for an exemption to the voluntariness obligation contains broad questions. Applicants are encouraged to provide fulsome and accurate information, with reference to the assessment factors, to enable the Regulator to efficiently assess their application. If the applicant provides minimal or inaccurate information, the exemption is less likely to be granted.

The assessment factors presented in Appendix A provide an indication of the range of factors that the Regulator may have regard to when considering an exemption from the voluntariness obligation. The list is not exhaustive, and the Regulator will consider each application on its merits, taking into account any matters relevant to a particular case.

Applicants will be given written notice of a decision to grant or to refuse to grant an exemption. If an exemption is granted, the Regulator may subsequently revoke it if it considers it appropriate to do so.

See section 74 of the Act for the requirements relating to exemptions.

9.4 Plans and procedures

Participating relying party applicants must have written procedures for notifying the System Administrator in the event:

- their IT system that interacts with the AGDIS changes in a material way
- an IT system outage (planned or unplanned) occurs that could have a material effect on the operation of the AGDIS.

See Rule 3.2 of the Digital ID Rules for the requirements relating to notifying the System Administrator.

Participating relying party applicants must have:

- conducted risk assessments to identify, evaluate and manage the risk of a cyber security incident and a digital ID fraud incident occurring in connection with a service that the organisation intends to provide, or provide access to, within the AGDIS.

See Rule 3.3(1) of the Digital ID Rules for the requirements relating to risk assessments.

- written plans that address:
  - cyber security
  - fraud management
  - disaster recovery and business continuity.

These plans must have been approved by the organisation's governing body and address the requirements in the Digital ID Rules.

The Regulator may request further information and documents as part of its assessment of this requirement.

When considering a streamlined application from a receiving entity (see section 9.5), the Rules do not require the Regulator to be provided with evidence of these plans and procedures on the basis that such evidence would have been previously provided by the transferring entity. However, it is open to the Regulator to request such evidence.

See Rule 3.3(2)(a–c) of the Digital ID Rules for the requirements relating to plans.

9.5 Participating Relying Parties affected by a Machinery of Government change.

A Commonwealth, State or Territory government participating relying party may be affected by a Machinery of Government (MoG) change. MoG changes can range from a simple change of name for a participating relying party to larger administrative changes, including the transfer of functions within a Ministerial portfolio or from one Ministerial portfolio to another.

If a participating relying party is affected by a MoG change that involves only a change of name, they can apply to the Regulator for a name change via the *Application to vary accreditation or AGDIS approval form* available on the Digital ID System website. See also the *Guidance for entities approved to participate in the AGDIS*.

However, if a MoG change involves, or is reasonably expected to involve, a transfer of functions that impacts a participating relying party's approval to provide, or provide access to approved service/s, the participating relying party receiving the service (receiving entity) is responsible for seeking approval from the Regulator to provide that service/s within the AGDIS. The entity that is giving up the function or service is called the transferring entity.

The *Digital ID Rules* allow for a streamlined application process for receiving entities affected by a MoG change. The streamlined process works to reduce the mandatory matters that must be considered by the Regulator in approving a relying party to participate in the AGDIS in all the relevant circumstances.

There are still factors that the Regulator must consider when assessing a streamlined application, such as whether the transferring entity has had its approval to participate suspended or revoked. In addition, the Regulator may exercise its powers under the Digital ID legislation to determine whether it is appropriate to approve the receiving entity.

If a participating relying party believes they may be affected by a MoG change, either as a transferring or a receiving entity, contacting the Regulator as early as possible is recommended. Early engagement allows time for discussion and coordination to make the process as smooth and streamlined as possible to prevent disruption to services. Engaging with the Regulator as soon possible will also help reduce risk of non compliance.

If an entity believes they may be affected by a MoG change, they are encouraged to notify the Regulator as soon as possible as this would be regarded as a material change.

See 1.5 of the Digital ID Rules for the meaning of streamlined application.

10. Review of Regulator decisions

Certain decisions of the Regulator are reviewable. This includes decisions of the Regulator to:

- refuse to approve an entity to participate in the AGDIS
- impose, vary or revoke a condition, or refuse to impose or vary a condition
- suspend or refuse to suspend an entity's approval to participate in the AGDIS
- revoke the AGDIS approval of entity.

A reviewable decision is eligible for internal review if it is made by a delegate of the decision maker. Other reviewable decisions are only eligible for review by the Administrative Review Tribunal or Federal Court (see below).

When the Regulator (the decision maker) advises an entity of the outcome of a decision, the Regulator's correspondence to the entity will include information on whether the decision by the Regulator is eligible for internal review or review by the Administrative Review Tribunal or Federal Court.

See Chapter 9, Part 4 of the Act for information about reviewable decisions.

10.1 Internal review

An application for internal review must be in writing and be made within 28 days after the day the decision first came to the notice of the entity. A request for review of a decision made by the Regulator must be made by the affected entity.

An entity can submit a written request for internal review via email to the Regulator at DigitalIDRegulator@accc.gov.au.

The Regulator is required to make an internal review decision to either uphold, vary or revoke the original decision within 90 days of receipt of the request for review.

The entity will be notified by the Regulator of the outcome of the internal review. If the Regulator's decision is to revoke the decision under review, the Regulator may make any other decision considered appropriate. The Regulator will provide the entity with a written statement of its reasons for its decision.

10.2 Review by the Administrative Review Tribunal

A reviewable decision will be eligible for external review by the Administrative Review Tribunal if the decision was made by the decision-maker personally (i.e. not a delegate), or if the decision is an internal review decision made by the Regulator.

The Regulator will advise the applicant if the decision is eligible for external review by the Administrative Review Tribunal. An application to the Administrative Review Tribunal for review of a reviewable decision made by the Regulator must be made by the entity affected by the reviewable decision.

Information on applying to the Administrative Review Tribunal for a review of a decision is available on the Administrative Review Tribunal website.

Refer to the factsheet *Internal review of a Digital ID Regulator Decision* on the Digital ID System website for additional details.

10.3 Judicial review

Applicants or approved entities may apply to the Federal Court for judicial review of certain decisions made by the Regulator. Judicial review is concerned only with the legality of the decision and is limited to questions of law, such as:

- whether the Regulator had the power to make the decision
- whether the decision-maker took an irrelevant consideration into account or failed to take a relevant consideration into account
- whether the decision was so unreasonable that no reasonable decision-maker could have made it.

Applicants may appeal to the Federal Court for judicial review of any decision of the Administrative Review Tribunal. Again, the Federal Court can rule only on questions of law, not on the merits of the decision.

Information on the process to apply to the Federal Court for judicial review of a decision is on the Federal Court of Australia website.

11. Following approval to participate

11.1 Participation start date

If an organisation's application to participate in the AGDIS is granted, it will be notified by the Regulator of the approval date and a participation start date. The organisation must begin participating in the AGDIS on its participation start date. Failure to commence participation on the organisation's participation start date will be non-compliance and may result in enforcement action.

The Regulator will coordinate the participation start date with the approved entity, the System Administrator and other entities already participating in the ADGIS.

If an approved entity is unable to start participating on its participation start date or becomes aware of issues which may impact its start date, it must notify the Regulator as soon as possible by submitting the *Application to vary participation start date for AGDIS approval*, available on the Digital ID System website.

11.2 AGDIS Register

All entities approved to participate in the AGDIS will be added to the AGDIS Register. The AGDIS Register is a public register available on the Digital ID System website and the ACCC Website.

The AGDIS Register will be updated to reflect any changes to an entity's approval or conditions, as well as organisation names, service names, and any suspensions or revocations of approval. If an entity's approval to participate in the AGDIS is revoked, the information will remain on the AGDIS Register for 3 years after the day on which the revocation came into force.

Section 121 of the Digital ID Act details what the AGDIS Register must contain for each organisation.

11.3 Changes to AGDIS approvals

An approved entity may apply for changes to its approval, including:

- requesting the imposition, variation or revocation of a condition on its approval
- adding or removing services it is approved to provide, or provide access to, in the AGDIS
- requesting the variation, suspension or revocation of its AGDIS approval.

The Regulator may also, on its own initiative, suspend or revoke an entity's approval, impose new conditions, or vary or revoke an existing condition on an entity's approval.

The Regulator must also suspend or revoke an entity's approval if the Minister for Finance directs it to do so for reasons of security (within the meaning of the *Australian Security Intelligence Act 1979*), including because of an adverse or qualified security assessment in respect of a person. See *Guidance for entities approved to participate in the Australian Government Digital ID System* available on the Digital ID System website for more detailed information on these processes.

12. Compliance obligations

Approved entities participating in the AGDIS have continuing compliance, disclosure and reporting obligations under the Digital ID legislation.

These obligations include:

- complying with the conditions that apply to the approved entity, including:
- participating only as the kind of entity it has been accredited and approved to participate as
- notifying the Regulator before adding new digital ID services or removing services (see sections 6.3 and 11.3)
- collecting and storing pairwise identifiers, where required
- ensuring that the entity's approved services are secure, easy to use, voluntary, accessible, inclusive and reliable
- complying with restrictions on collection of restricted attributes of individuals (relevant to participating relying parties)
- notifying the Regulator or System Administrator of reportable incidents
- maintaining comprehensive records as required by the Act

In addition, an entity must ensure that any representation it makes concerning its accreditation or approval status under the Act is accurate, and not misleading or deceptive.

An accredited entity, including one that is participating in the AGDIS, may only use and display the Digital ID Accreditation Trustmark in accordance with the requirements prescribed in the Act and Digital ID Rules. Such an organisation must also ensure that its use of the Digital ID Accreditation Trustmark complies with the Australian Consumer Law.

Failure to meet compliance obligations may result in **enforcement action** by the Regulator, including litigation seeking *injunctions* and/or substantial *civil pecuniary penalties* in appropriate cases.

This guidance contains a summary of some of the key obligations of approved entities, including:

- record keeping obligations
- reportable incident obligations
- obligations under the AGDIS Redress framework.

Approved entities should refer to the *Guidance for entities approved to participate in the Australian Government Digital ID System* available on the Digital ID System website which details key responsibilities of approved entities.

This guidance contains general information about the obligations of approved entities. It is not legal advice and is not a comprehensive or exhaustive statement of all obligations approved entities must comply with. Organisations should seek their own professional advice about the Digital ID legislation.

12.1 Record keeping obligations

Approved entities must comply with the obligations prescribed in the Digital ID Rules that require prescribed records to be kept for at least 3 years or as otherwise prescribed.

In addition, approved entities must comply with destruction or de-identifying of personal information in their possession or control that was obtained though the AGDIS. Non-compliance with these obligations is enforced by the OAIC.

These obligations are civil penalty provisions under the Act with substantial pecuniary penalties.

See sections 135 and 136 of the Digital ID Act and Chapter 6 of the Digital ID Rules for the record keeping obligations.

12.2 Reportable incident obligations

Approved entities have obligations to report certain incidents that have occurred, or are reasonably suspected to have occurred, in connection with the AGDIS, within specified timeframes.

Some of these reporting requirements involve notifying the Regulator, while others require notifications to be made to the System Administrator. The following are examples of notification requirements for reportable incidents that approved entities must comply with:

Notifications and reportable incidents	
Notifications to the System Administrator	▪ Cyber security incidents. ▪ Digital ID fraud incidents. – If the System Administrator directs an entity to conduct an investigation into a notified cyber security or Digital ID fraud incident, the entity must: • commence the investigation • provide the System Administrator with a summary of the findings of the investigation as soon as reasonably practicable after the investigation is complete. – If an investigation is not complete within 28 days of the direction, the entity must update the System Administrator on the progress of the investigation: immediately after the end of that period and at least once after the end of any subsequent 28 day period until the investigation is complete. ▪ Proposed changes to information technology systems that interact with the AGDIS if the change could reasonably be expected to have a material effect on the operation of the AGDIS. ▪ Any planned or unplanned outage or downtime affecting the entity's IT system that could reasonably be expected to have a material effect on the AGDIS.

Notifications and reportable incidents	
Notifications to the Regulator	▪ Any material changes in the organisation's circumstances that may affect its ability to comply with its obligations under the Digital ID legal framework. ▪ Any matters that could reasonably be considered relevant to a decision as to whether the organisation, or an associated person of the organisation, is a fit and proper person for the purposes of the Digital ID legal framework. ▪ Any material changes to, or error in, any of the information provided to the Regulator. An accredited entity participating in the AGDIS must also notify the Regulator if it proposes to use an IT system that it uses to provide services within the AGDIS to provide or receive services within a digital ID system other than the AGDIS. A participating relying party also needs to comply with a condition imposed by the rules to notify the Regulator of proposed changes to its contact details.

If an entity believes they may be affected by a MoG change (see section 9.5) they are encouraged to notify the Regulator as soon as possible as this would be regarded as a material change.

To notify the Regulator of a reportable incident, entities must email the Regulator directly at DigitalIDRegulator@accc.gov.au. The email subject line should clearly specify the type of incident and that it constitutes a mandatory report.

Failure to comply with certain notification requirements may result in enforcement action, including substantial civil pecuniary penalties.

These reporting obligations also apply to a participating entity whose approval is suspended in respect of reportable incidents that occurred or are reasonably suspected to have occurred while the entity was participating in the AGDIS.

See Chapter 4 of the Digital ID Rules for the reportable incidents and notification requirements.

12.3 Obligations under the AGDIS Redress framework

An AGDIS Redress framework has been developed to support individuals affected by digital ID fraud and cyber security incidents that occur in relation to accredited services provided by identity service providers and attribute service providers within the AGDIS.

Notifying affected individuals

If an identity service provider or attribute service provider experiences or reasonably suspects a cyber security incident or a digital ID fraud incident has occurred in relation to one of their accredited services within the AGDIS, they must make reasonable attempts to notify each individual affected by the incident.

This requirement will not apply if the Identity Service Provider or Attribute Service Provider is satisfied that:

1. it is likely the individual will suffer an adverse outcome because of the attempt to notify, or
2. notification would, or could reasonably be expected to, have a material effect on the AGDIS. From 30 September 2026 entities must consider whether notification would have a significant impact on the AGDIS (rather than a material effect).

Also from 30 September 2026, as part of the notification requirements, entities must **not** give regard to the effect the notification might have on the entity in relation to the following:

- whether notifying the individual might result in embarrassment or reputational damage
- attract media attention
- increase administrative costs or administrative burden, or
- be related to compliance or enforcement action being taken, or that might be taken, by the Digital ID Regulator or the Information Commissioner against the entity.

From 30 September 2026, entities will also need to keep records of when an entity has decided not to notify an affected individual. See rule 4A.2 (4) and (5) for further details.

Provision of information, support and assistance to individuals

An identity service provider or attribute service provider is required to provide information, support and assistance to individuals affected by:

- a digital ID fraud or cyber security incident about which they have been notified
- a technical issue about which an individual has made a complaint.

Referrals to the System Administrator

If a cyber security or fraud incident has occurred, or is reasonably suspected of having occurred, and it gives rise to a technical issue that prevents an individual from using their digital ID, the identity service provider or attribute service provider must refer the incident to the System Administrator if it is reasonably satisfied that:

- it cannot resolve the problem without referring the matter, and
- it has provided all necessary information, support and assistance to individuals affected by the incident.

The identity service provider or attribute service provider must refer the incident to the System Administrator:

- as soon as reasonably practicable after becoming aware of the issue, and
- in any case within 28 days if the issue is raised because of a complaint made by an individual.

This responsibility is in addition to, and does not replace, the obligation to notify the affected individual as outlined above.

Recommendations and directions from the System Administrator

If an entity refers an incident to the System Administrator, the System Administrator may currently recommend certain courses of action to resolve a technical issue. From 30 September 2026, the System Administrator's powers to recommend certain courses of action will change slightly. A recommendation from the System Administrator may be to either recommend a course of action to resolve the technical issue, and/or to pay an amount to the affected individual.

Furthermore, an entity will need to give the System Administrator a notice specifying whether it proposes to implement a recommendation from the System Administrator, and if it does not propose to implement the recommendation, reasons why.

From 30 September 2026, the requirement to notify the System Administrator about whether an entity proposes to implement a recommendation will form a condition of the entity's approval. If the System Administrator makes a recommendation to an entity, the System Administrator will provide the Regulator with details of the recommendation.

From 30 September 2026, the System Administrator will also have the power to give a direction to an entity to take action in response to the technical issue. The System Administrator may provide a direction to require the entity to either provide an explanation of the circumstances giving rise to the technical issue and/or to issue an apology to the affected individual.

A direction from the System Administrator also forms a condition on an entity's approval and will be reported to the Regulator by the System Administrator.

After 30 September 2026, an entity must comply with a direction by the System Administrator under subrule 4A.3A(2). An entity must also comply with subrule 4A.4(4) if it is given a recommendation under subrule 4A.4(1)

Redress policies and publications

From 1 July 2026, identity service providers or attribute service providers (that have not had their approval to participate suspended or revoked) must have in place published policies related to:

- the identification, management and resolution of cyber security incidents and digital ID fraud incidents that occur, or are reasonably suspected of having occurred, in relation to their accredited services in the AGDIS
- complaints by individuals relating to cyber security incidents and digital ID fraud incidents that occur, or are reasonably suspected of having occurred, in relation to their accredited services in the AGDIS.

At a minimum the complaints policy/s must deal with the following:

- how an individual can make a complaint to the entity, including relevant contact details
- the procedure the entity will follow to deal with and investigate complaints
- a simple outline of the procedures, and
- the timeframe within which an individual can expect their complaint to be resolved.

An entity does not need to create a new digital ID specific complaints policy/s, however they must cover the necessary matters required under the legislation and be published in a way to maximise public access.

See part 5 of Chapter 4A of the Digital ID Rules for further details on policies relating to incidents and complaints

Appendix A – Exemption application assessment factors

The Regulator will generally only grant exemptions to the voluntariness obligation in exceptional circumstances.

The following table lists the assessment factors the Regulator may consider in determining applications for exemptions.

Factor	Information to be provided by applicants
The type of applicant and services	
Whether the applicant is eligible for an exemption to the voluntariness obligation. The Regulator cannot grant an exemption to: ▪ a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013* (Cth) ▪ a person or body that is an agency within the meaning of the *Freedom of Information Act 1982* (Cth) ▪ a body specified, or the person holding an office specified, in Part I of Schedule 2 to the meaning *Freedom of Information Act 1982* (Cth).	
Whether the applicant is a small business. Being a small business does not guarantee that an exemption will be granted. The applicant must demonstrate why its circumstances are exceptional and justify an exemption being granted.	Provide details of the applicant's organisation type and the number of employees, annual revenue and other factors relevant to the business size.
Whether the applicant provides services, or access to services, solely online. Providing services solely online will not guarantee that an exemption will be granted. The applicant must demonstrate why its circumstances are exceptional and justify an exemption being granted.	Provide details of the channels the applicant uses to provide products and services to its consumers.
Impact of proposed exemption on the applicant, consumers and the AGDIS	
Whether the applicant has explored alternative options to facilitate compliance.	Provide details of alternative options the applicant explored to facilitate compliance with the voluntariness requirement and why these are not viable.
Whether the proposed exemption is only required for a limited time.	Provide details of the scope and duration of the proposed exemption. For example, is the proposed exemption for a limited time in response to a specific event, such as an emergency situation?
Potential for any perverse consequences for the applicant, consumers or the AGDIS if the exemption is not granted.	Provide details of risk of negative consequences to the applicant, consumers or the AGDIS if the exemption is not granted, including the likelihood and impact of the risk/s eventuating.

Factor	Information to be provided by applicants
The number of consumers potentially affected if the exemption is granted. The more consumers affected, the less likely the exemption will be granted.	Provide details of the market/s the applicant provides services to, and the number of consumers expected to access the service/currently accessing the service. Provide details of the number of consumers expected to access the service, or currently accessing the service, who are known to use a digital ID. Provide details of the number of consumers potentially impacted if the exemption is granted, and how they will be impacted.
Whether the exemption affects vulnerable consumers. The greater the impact to vulnerable consumers, the less likely the exemption will be granted.	Provide details of any vulnerable consumer groups who are expected to or currently access the service. Provide details of consideration the applicant has given to the impacts on vulnerable consumers if the exemption is granted and how these impacts will be managed.
Whether the exemption would unduly undermine access to services of that kind.	Provide details of the type and purpose of the service, including available alternatives to the applicant's provision of that service and the accessibility of those alternatives.
Whether the service directly or indirectly impacts other services and whether the exemption would directly or indirectly impact other services.	Provide details of whether the service directly or indirectly impacts other services. Provide details of whether the exemption would impact other services in the AGDIS. Provide details of any risk to other services in the AGDIS if the exemption is/is not granted.
Whether the applicant will otherwise meet its obligations under the Digital ID legislation	
Other conditions or exemptions sought or granted. Where granting the exemption may result in other conditions imposed by the Regulator being contravened, the exemption is less likely to be granted.	Provide details of any other conditions imposed on the applicant under the Digital ID legislation (including conditions being sought or expected to be sought) and their interaction with the exemption.
Compliance history. If the applicant has demonstrated a history of non-compliance, the exemption is less likely to be granted. However, a history of compliance does not guarantee the exemption will be granted.	Provide details of any incidents of non-compliance with the Digital ID legislation.
Proactive engagement with the Regulator. A lack of proactive engagement with the Regulator will make an exemption less likely to be granted. However, proactive engagement does not guarantee the exemption will be granted.	
Provided evidence and clear justification in support of the application.	Provide a clear justification, and evidence in support, for why the exemption should be granted.
Other	Provide details of any other factors that the applicant considers may be relevant to the Regulator's assessment of the exemption application.


AUSTRALIA


ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION