AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Applying for accreditation

Guidance for organisations seeking to become accredited in Australia's Digital ID System

Version 1
November 2024

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.

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

© Commonwealth of Australia 2024

This work is copyright. In addition to any use permitted under the *Copyright Act 1968*, all material contained within this work is provided under a Creative Commons Attribution 4.0 Australia licence, with the exception of:

- the Commonwealth Coat of Arms
- the ACCC and AER logos
- any illustration, diagram, photograph or graphic over which the Australian Competition and Consumer Commission does not hold copyright, but which may be part of or contained within this publication.

The details of the relevant licence conditions are available on the Creative Commons website, as is the full legal code for the CC BY 4.0 AU licence.

Requests and inquiries concerning reproduction and rights should be addressed to the General Manager, Strategic Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have any specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties who wish to re-publish or otherwise use the information in this publication must check this information for currency and accuracy prior to publication. This should be done prior to each publication edition, as ACCC guidance and relevant transitional legislation frequently change. Any queries parties have should be addressed to the General Manager, Strategic Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 11/24_24–79

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 to be an accredited Digital ID service provider with lodging a valid application for accreditation.

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 of this guidance. The website contains detailed information for applicants and approved entities, including the 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 accreditation, 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 accredited entities to have a full understanding of the Digital ID legislation (see section 2.1).

An accredited entity that wishes to participate in the AGDIS will also need to apply for approval to participate. The ACCC has prepared separate guidance on this. *See Applying for approval: guidance for organisations seeking to become approved in the Australian Government 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 System Administrator, the Office of the Australian Information Commissioner (OAIC) and the Data Standards Chair.

1.3 Communicating with the Regulator

All organisations that wish to make an application for accreditation 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.

Accredited 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.

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. Organisations are responsible for ensuring they familiarise themselves with these documents and understand their obligations.

	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 requirements entities must meet to become and remain accredited, including to manage fraud, security, privacy, accessibility, and useability, 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* and corresponding Explanatory Statement	These standards cover the technical requirements of 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.

2.2 Agency roles

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, and
- undertaking compliance monitoring and enforcement activities for non-privacy aspects of the Digital ID legislation.

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

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

- providing oversight of the new '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
- performing Notifiable Data Breach scheme functions in relation to the Digital ID System
- undertaking assessments of Digital ID System compliance.

The System Administrator is responsible for administering operational aspects of the AGDIS, including the security, 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. More information about the System Administrator's role in the AGDIS is in *Applying for approval: guidance for organisations seeking to become approved in the Australian Government Digital ID System*, available on the Digital ID System website.

The Data Standards Body supports the Digital ID Data Standards Chair on the implementation and operation of data standards for Australia's Digital ID System.

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. Accreditation under the Digital ID System

Organisations, including Commonwealth, state and territory departments, and private businesses, can apply to become accredited entities under the Digital ID legislation.

Accreditation allows organisations to demonstrate that their Digital ID services meet high standards in areas such as privacy protection, protective security, and fraud control.

Organisations can apply to the Regulator to become one (or more) of 3 kinds of accredited entities:

- **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, and
  - 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 data or other information between participants in the Digital ID System.

The AGDIS approval process allows eligible accredited entities and relying parties to apply to the Regulator to participate in the AGDIS. Relying parties are the organisations that provide a service, or access to a service, to consumers by verifying the consumer's identity or attributes through an accredited entity.

4. Application steps

4.1 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 accredited
  - the Authorised Officer for the organisation, 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 to be, or already accredited under the Act
  - the contact person/s for the service.

4.2 Accreditation application form

An organisation seeking accreditation within Australia's Digital ID System is required to use the Regulator's *Accreditation application form* (application form), available on the Digital ID System website. This form must be submitted to the Regulator with all required documents.

The application form has mandatory sections covering:

- general information about the organisation
- requests for conditions to be applied to the accredited service
- privacy requirements
- fraud requirements
- protective security requirements
- details related to accessibility and useability.

The application form contains additional sections specific to the service type (i.e. identity service provider, identity exchange provider, or attribute service provider) or characteristics of the accreditation being sought (e.g. identity proofing level, intended use of biometric information or alternative proofing processes). Applicants are only required to answer questions relevant to their application.

The application form lists documents that applicants should provide to satisfy the Regulator that they are able to comply with the legislative requirements. Where the application form indicates a document is mandatory, it must be provided. The documents listed in the application form include documents required by the legislation to be provided to the Regulator, and documents that are likely to be held by the applicant. Applicants may also submit additional evidence to demonstrate they can meet applicable requirements.

The application form also contains a section addressing evidence that it is appropriate to accredit the organisation. Applicants should consider the information in section 7 and then complete the separate *Evidence it is appropriate to accredit or approve the organisation form* (evidence of appropriateness form), available on the Digital ID System website. The completed form and supporting evidence should be submitted to the Regulator as part of the application for accreditation.

A list of the documents requested or mandated in the application form is available in Appendix B.

A submitted application will be subject to a completeness check prior to being accepted by the Regulator for the purposes of assessing the application (section 5 lists the steps in the assessment process).

Once the Regulator has assessed the information submitted in an application, it will decide whether to accredit or refuse to accredit the organisation.

Section 15 of the Act details the Regulator's obligations regarding accreditation decisions.

4.3 Completing an application

For the Regulator to assess an application for accreditation, the applicant must have submitted the completed application to the Regulator with all required documents. In summary, the applicant will be required to provide:

- the completed *Organisation and Authorised Officer* form and *Service and Contact Person form* (as detailed in section 4.1)
- the completed application form (as detailed in section 4.2)
- evidence in support of the application, including evidence in support of any conditions requested
- a completed evidence of appropriateness form (as detailed in section 4.2) and associated documentation
- a completed *Declaration for entities seeking accreditation form* that confirms they understand their legal obligations under the Act, Rules, and Data Standards (available on the Digital ID System website) and associated documentation.

5. Regulator's assessment

5.1 Completeness check

Prior to accepting an application for accreditation, the Regulator will carry out a 'completeness check' to verify that:

- the statement of scope and applicability is accurate
- the documents provided are consistent with the applicant's stated DI data environment (detailed in section 8.1)
- all necessary information and documents have been provided and address the legislative requirements
- assessors providing privacy impact assessments, assurance assessments and systems testing reports are appropriately experienced and qualified.

5.2 Assessment

If an application is complete, it will proceed to the assessment stage. If the Regulator identifies any gaps or deficiencies during the completeness check, it will advise the applicant and identify the issues requiring rectification prior to re-submission.

The Regulator may request further information from an applicant at any stage during the assessment process. The Regulator may also consult or share information with other Australian Government authorities such as the OAIC, national security agencies, or similar authorities overseas.

5.3 Decision

The Regulator will advise applicants in writing of its decision to grant, or not to grant, accreditation.

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

6. Conditions on accreditation

6.1 Accreditation is subject to conditions

An accredited entity must comply with the conditions imposed on its accreditation. Failure to comply with imposed conditions may result in suspension or revocation of accreditation.

Conditions may be imposed at the time of accreditation or at a later stage. Accreditation is also subject to several default conditions which are set out in the Digital ID legislation (detailed in section 6.3).

Conditions on an entity's accreditation and approval to participate in the AGDIS do not necessarily have to be the same, meaning that an accredited entity participating in the AGDIS may have separate conditions on its accreditation and approval. However, conditions applying to participants in the AGDIS cannot be more permissive than the conditions the entity holds as an accredited service provider.

6.2 Conditions requested by an applicant

In the application form, applicants can request that conditions relevant to their accreditation be imposed by the Regulator.

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 the applicant will comply with the condition.

For example, if an applicant seeks to conduct an alternative proofing process, it will be required to apply for a condition that authorises this. Examples of the kinds of supporting evidence expected for this kind of condition include:

- details of the proposed alternative proofing process
- evidence that an exceptional use case exists in respect of individuals proposed to undertake an alternative proofing process
- a risk assessment in relation to the proposed alternative proofing process, including of the risks to relying parties that may rely on the individual's digital ID, if created
- a report of the risk assessment, including details of the controls and risk mitigation strategies to be implemented in response to the identified risks.

Accredited entities can also apply for a condition to be imposed after being accredited, as well as apply to vary or revoke a condition. See section 11.3 for information about the application process for a condition to be imposed, varied or revoked.

6.3 Default conditions

All accredited entities are subject to default conditions which are applied by the Act, the Digital ID Rules, and the Accreditation Rules, depending on the kind of accredited services being provided.

Default conditions include that accredited entities must comply with:

- all legislative requirements
- requirements in the Digital ID Rules relating to the use and display of the Digital ID Accreditation Trustmark
- requirements in the Accreditation Rules, including in relation to the collection and disclosure of restricted attributes and biometric information of individuals.

See sections 16-19 of the Digital ID Act and Part 7.2 of the Accreditation Rules for information about conditions

6.4 Conditions imposed by the Regulator or Minister

Additional conditions can also be imposed by the Regulator on its own initiative if it considers it appropriate in the circumstances. These conditions can be imposed at the time of accreditation, or at any other time. The Regulator will provide an entity with notice of a condition it proposes to impose, unless the Regulator considers the condition is serious and urgent.

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

6.5 Categories of conditions

The Regulator has a broad power to impose conditions (including those requested by applicants), which fall into 3 main categories.

1. Conditions to define the scope of accredited services

The Regulator will impose conditions to define the scope of the accredited services, as well as declare the features and behaviours that a service may or must have and the circumstances or way these services must be provided.

Types of conditions that fall under this category include but are not limited to:

- the features of the accredited service (i.e. identity proofing levels, authentication levels, reusable or one-off digital ID)
- the circumstances or manner in which the accredited services must be provided
- any limitations, exclusions or restrictions in relation to the accredited service.

2. Condition to authorise certain conduct

The Regulator may impose conditions to authorise accredited entities to engage in certain conduct that would otherwise be prohibited or restricted under the Act.

Types of conditions that fall under this category include but are not limited to:

- whether the accredited entity is authorised to collect or disclose a restricted attribute of an individual (e.g. health information, information about a criminal record, or an identifier of an individual contained on a government issued document)
- whether the accredited entity is authorised to collect, use or disclose the biometric information of an individual
- whether the accredited entity is authorised to perform an alternative proofing process.

3. Conditions to direct certain conduct

The Regulator may impose conditions to direct accredited entities to engage in certain conduct or take certain actions.

Types of conditions that fall under this category include but are not limited to:

- directing an entity to take certain actions before suspending or revoking the entity's accreditation or 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.

7. Appropriateness to accredit

Before approving an application for accreditation, the Regulator must be satisfied it is appropriate to accredit the organisation in light of the objects of the Act, which include promoting privacy, the security of personal information, and trust in digital ID services among the Australian community.

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

To assist this determination, applicants for accreditation must complete the evidence of appropriateness form (discussed in section 4.2) and submit the form and associated documents to the Regulator. The evidence of appropriateness form is available on the Digital ID System website.

The evidence of appropriateness form enables an organisation to demonstrate it is appropriate for the Regulator to accredit 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.

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

7.1 Fit and proper person test or alternative evidence

When deciding whether to accredit 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).

Due to the broad range of organisations that may seek accreditation, 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 accredit the organisation. 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 accredit 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 another similar fit and proper person test**.

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 accredit 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 accreditation.

7.2 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 Person 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 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 management of the organisation's DI data environment or have the capacity to significantly affect the management of the DI data environment. 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 DI data environment and accredited services
  - any other staff who have influence over the work that could significantly affect or influence the management of the DI data environment, and
  - 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.

7.3 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 accredit 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 organisation's management of its DI data environment.

To the extent any of this information has been provided in response to other sections of the 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 organisation's management of its DI data environment, 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 alternative 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 accredit 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.

7.4 Ongoing reporting requirements

Accredited 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 accreditation.

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

See rule 7.4(b) in the Accreditation Rules for more information.

8. Accreditation criteria and evidence requirements

To accredit an applicant, the Regulator must be satisfied that the organisation:

- can comply with all relevant legislative requirements
- has correctly defined and documented the boundaries of its DI data environment, and has limited it to the extent practicable
- has provided all information and documentation required to accompany an application for accreditation
- has an operational information technology (IT) system through which it will provide its accredited services
- has conducted each kind of assessment and testing required by the Accreditation Rules and Accreditation Data Standards (see section 9).

In deciding whether to accredit an applicant, the Regulator must also have regard to the level of the applicant's tolerance for fraud and cyber security risks, and whether the applicant's risk tolerance level is likely to create an unacceptable risk if accredited. An applicant's protective security assessment and fraud assessment, and its responses to risks identified in those reports, including risk mitigation strategies, will be particularly important to the Regulator in making this judgment.

The Regulator must also consider whether the applicant's privacy impact assessment and response identify any matters that may give rise to an unacceptable risk to the privacy of individuals.

See rule 2.6 in the Accreditation Rules for more information on matters that the Regulator must consider in deciding whether to accredit an applicant.

8.1 DI data environment

The Regulator must not accredit an applicant unless it is satisfied that it has correctly identified and documented the boundaries of its DI data environment and has limited the boundaries of that environment to the extent practicable.

See rules 1.4 and 2.1 in the Accreditation Rules for the requirements relating to DI data environment.

The DI data environment means the IT systems used for, and the processes that relate to, the provision of an organisation's proposed accredited services. An applicant must define the boundaries of its DI data environment, including the people, processes, technology and infrastructure through which the proposed accredited services are provided. Each applicant's DI data environment will be different, subject to factors including what kind of supply chain it operates, use of third-party contractors, and the delivery (mobile, website or in-person) of these services.

A well-defined DI data environment is an important reference document for the Regulator, assessors, and the applicant itself to understand exactly where the boundaries of the proposed accredited services lie.

It is critical that an applicant demonstrates to the satisfaction of the Regulator that the DI data environment documentation:

- clearly defines the scope and boundaries of its proposed accredited services
- specifies any infrastructure owned or managed by contractors
- segregates the environment, to the extent practicable, from other systems and minimises the number of people (including contractors) or systems hosting, processing or accessing information generated, collected, used, held or disclosed for the purpose of providing the proposed accredited services.

Defining the DI data environment is particularly important where an accredited entity uses the same infrastructure, IT systems and/or contractors, in whole or in part, for both accredited and unaccredited services. The Digital ID legislation will apply whenever an accredited entity collects, generates, uses, holds, or discloses information for the purpose of providing an accredited service.

To satisfy this requirement, documentation of the DI data environment should include:

- a narrative description and illustrative diagrams for the proposed accredited service
- identification of the proposed accredited service's boundary and information flows and interfaces. This would include data transmission, data in use, internal transmission (i.e. audit trails, event logs, disclosure to third parties)
- key infrastructure and software required for operation/support of the proposed accredited service, including major versions and data storage (back-ups, repositories, caches etc.)
- key people involved in the operation and development of the proposed accredited service and their location (branch, department etc.) in the organisation. An organisational chart is helpful context, especially reporting lines/escalation pathways
- significant third parties supporting the development or operation of the proposed accredited service (e.g. cloud service providers, managed service providers, physical security services, critical design and delivery partners etc.)
- key evidence documents supporting the operation of the proposed accredited service (procedures, plans etc.).

8.2 Statement of scope and applicability

An applicant must provide a statement of scope and applicability that lists:

- each requirement in the Accreditation Rules and the Accreditation Data Standards with which the applicant must comply in relation to its proposed accredited services, and
- the evidence that demonstrates that the applicant complies with those requirements or will comply if accredited.

See rules 1.4 and 2.2 in the Accreditation Rules for the requirements relating to the statement of scope and applicability.

While the Accreditation Rules do not mandate the form of the statement of scope and applicability, an applicant may find it useful to submit a spreadsheet detailing the requirements and corresponding evidence that demonstrates compliance. Where an applicant's evidence is more than one document, or contains other information, it would be useful to pinpoint the sections that demonstrate compliance with the relevant legislative requirement.

8.3 Privacy impact assessment

An applicant must provide a privacy impact assessment that assesses compliance against the privacy requirements in the Act and the Accreditation Rules, and that provides analysis of the privacy impacts of the proposed accredited services.

A privacy impact assessment should include analysis of how an applicant's proposed services will impact the privacy of individuals and protection of personal information, if accredited. An assessment report should include any recommendations by the assessor, including recommendations that the applicant undertake activities to mitigate any identified privacy risks.

A privacy impact assessment must be undertaken by an assessor with relevant experience, training and qualifications (see Appendix A). The assessor must be external to the organisation and must not have been involved in the design, implementation, operation or management of the applicant's DI data environment or accredited services.

A privacy impact assessment will include an assessment of the relevant documentation, processes and mechanisms that facilitate an applicant's ability to comply with the relevant privacy requirements (e.g. privacy management plans, privacy policies and data breach response plans). These underlying documents must be submitted with an application for accreditation.

See rule 2.4 in the Accreditation Rules for the requirements relating to privacy impact assessments.

An applicant must:

- respond in writing to the findings and recommendations in the privacy impact assessment, with the response signed by the entity's accountable executive (an organisation's accountable executive is a senior executive responsible for the overall management of the organisation's DI data environment and proposed accredited services)
- conduct a risk assessment and assign a rating for each risk and recommendation identified against the applicant's risk matrix, which must be based on an established risk management framework, or standard
- respond to each risk or recommendation identified by an assessor. An applicant's response to each risk will be determined by the risk rating and must include details of the actions to address the risk, timeframes for completion of actions, and the residual risk following completion of the planned action.

8.4 Technical testing

Applicants are required to verify that the information systems through which an entity will provide its accredited service includes and can execute the necessary functionality to support the kind of accredited service(s) that the entity is seeking to be accredited for. This technical testing should be appropriately scoped based on the features and behaviours of the proposed accredited service(s) and the statement of scope and applicability.

Entities seeking accreditation are required to undertake technical testing to determine whether their systems have the functionality necessary to meet the requirements within the Accreditation Rules and Accreditation Data Standards, including the following:

- Cyber security incident monitoring, detection, investigation, management, and response.
- Logging requirements.

- Fraud incident monitoring, detection, investigation, management, and response.
- User support requirements.
- Data minimisation requirements.
- Compliance with the relevant Accreditation Data Standards.

When applying for accreditation, applicants are required to provide:

- a statement, signed by the applicant's accountable executive, attesting that:
  - the technical testing has been conducted
  - the accountable executive is satisfied the results of the technical testing demonstrate that the requirements are met
    - The *Declaration technical testing attestation statement for entities seeking accreditation form* is available on the Digital ID System website
- for applicants required to conduct biometric testing, a copy of the reports of the testing and any required responses to the reports.

The application form also requests evidence of technical testing which refers to the information an applicant is required to provide under subrule 2.5(3) of the Accreditation Rules. An applicant is required to record:

- the test completion criteria used
- the assumptions, limitations and dependencies used
- the methodology used
- how each test conducted maps to each requirement that the applicant's IT system must meet
- the results of the technical testing.

Applicants should consider how to best provide this evidence to the Regulator. A requirements traceability matrix is an example of how this information may be provided.

Technical testing attestation statement

The technical testing attestation statement attests that the required technical testing has been conducted and the accountable executive is satisfied the results of the testing demonstrated the organisation will meet the relevant legal requirements, if accredited. If the applicant uses a cloud service provider within its DI data environment, additional legislative requirements necessitate that the penetration testing has been conducted by the cloud service provider rather than the applicant in some circumstances.

Applicants should utilise the *Declaration technical testing attestation statement for entities seeking accreditation form* (available on the Digital ID System website) to attest the technical testing requirements have been met.

See rule 2.5 in the Accreditation Rules for the requirements relating to technical testing.

Applicants have additional record keeping requirements relating to the technical testing they conduct. The Regulator may request these records as part of its assessment.

8.5 Biometrics

An applicant seeking to be accredited as an identity service provider conducting identity proofing at levels IP2 Plus or higher, is required to:

- demonstrate an ability to meet the relevant biometric requirements in the Act and in Chapter 5, Part 5.1, Division 2, Subdivision B of the Accreditation Rules, and
- provide copy of reports of the biometric testing conducted in accordance with the Accreditation Data Standards.

Personnel conducting biometric testing must have appropriate experience in conducting biometric testing, must be external to the applicant, and must not have been involved in the design, implementation, operation or management of the applicant's DI data environment or accredited services.

See data standard 2.2 of the Accreditation Data Standards for information about the Biometric testing entity.

Additional biometric requirements

Applicants that propose biometric capabilities as part of their application must be aware of the additional privacy safeguards in relation to the collection, use, disclosure, and destruction of biometric information, outlined Chapter 3, Part 2, Division 2 of the Act.

Applicants seeking to use biometric information for testing activities must ensure that they are compliant with the relevant rules in Chapter 4, Part 4.5 of the Accreditation Rules, including that:

- the testing is conducted in accordance with the purposes and circumstances in which testing may be conducted
- the testing is conducted in accordance with the requirements of policies covering the ethical use of biometric information to ensure biometric systems do not selectively disadvantage or discriminate against any group, and
- for each reporting period, prepare a report detailing the results of any testing using biometric information.

Applicants seeking to use biometric information for fraud activities must ensure that their digital ID fraud risk management activities have been conducted in accordance with written ethical principles aimed at avoiding disadvantage to, or discrimination against, individuals.

Applicants should consider whether a condition is required to authorise the collection, use, and disclosure of biometric information for the intended purposes. If so, applicants should also apply for any relevant conditions, unless already authorised by a default condition.

9. Assurance assessments and systems testing

An organisation applying for accreditation must have conducted all assurance assessments and systems testing as required by the Accreditation Rules and Accreditation Data Standards.

The results of the assessments and testing help demonstrate to the Regulator that the applicant will be able to comply with the relevant legislation, if accredited. The findings and recommendations are also key to the Regulator's consideration of whether there are likely to be unacceptable fraud or cyber security risks, or risks to the privacy of individuals, if an applicant is accredited.

The required assurance assessments and systems testing must be conducted having regard to the relevant requirements from the Accreditation Rules and Accreditation Data Standards (as detailed in the applicant's statement of scope and applicability), and in respect of the applicant's DI data environment at the time of the assessment.

See Chapter 3 in the Accreditation Rules for the requirements relating to assurance assessments and systems testing.

9.1 Reports for assurance assessments and systems testing

For each assurance assessment or systems test, an assessor must prepare a report that meets the requirements of the Accreditation Rules, including but not limited to:

- details of the testing
- details of the evaluation or test methodology used
- the assessment findings, including details of any relevant non-compliance, risks identified and treatments
- the qualifications and experience of the assessor.

An applicant must:

- respond in writing to the findings of each assessor report and the response must be signed by the organisation's accountable executive
- conduct a risk assessment against a risk matrix for each risk and recommendation identified in an assessor's report, based on an established risk management framework
- assign a risk rating in accordance with the risk matrix and respond to each risk identified in the assessor's report as requiring treatment and to each recommendation in the report
- detail the action it will take to implement the treatment or recommendation, the timeframe in which it will complete the action, and the expected residual risk rating following the action for each risk and recommendation accepted.

Where an applicant does not accept a risk or recommendation, it must set out the reasons for the non-acceptance, detail any alternative actions to be taken and associated timeframes, and the expected residual risk rating following the alternative action.

Applicants have flexibility to implement an established risk management framework that is relevant to them and appropriate for their industry. The Accreditation Rules Explanatory Statement provides examples of established risk management frameworks.

See Part 3.4 in the Accreditation Rules for the requirements relating to reports for assurance assessments and systems testing.

9.2 Assessor requirements

The role of independent assessors is critical in providing assurance to the Regulator that an applicant will be able to comply with the relevant legislative requirements under the Act, Digital ID Rules, Accreditation Rules, and Accreditation Data Standards.

It is the responsibility of an applicant to demonstrate to the Regulator that all required assurance assessments and systems testing has been conducted by an individual who:

- has the appropriate experience, training and qualifications to undertake the required assessment
- meets any additional requirements in the Accreditation Rules for the specific assessment or testing undertaken.

For assessors undertaking fraud assessments, penetration testing, privacy impact assessments and protective security assessments, the Accreditation Rules require that the assessor is external to the applicant and, if applicable, external to the applicant's corporate group. The Accreditation Rules also require that the assessor has not been involved in the design, implementation, operation or management of the applicant's accredited services or DI data environment.

Details of the experience, training and qualifications of the assessor must be included with each required assurance assessment and systems testing. This may include relevant and currently maintained certifications, a current curriculum vitae, and any registrations with relevant bodies. Applicants should consider relevant industry standards in deciding whether an assessor is appropriate for a particular assessment or test.

For assessments or testing where there is no specific requirement in the Accreditation Rules for an assessor to be external to the organisation, an applicant could consider providing evidence that there is no conflict of interest. This evidence could take the form of an independence statement or similar.

Appendix A in this guidance contains more detailed information about assessor qualifications.

See rule 3.2 in the Accreditation Rules for assessor requirements.

9.3 Assurance assessments

Protective security assessment

The protective security assessment must review and assess the applicant's implementation of, and compliance with, the controls in the protective security framework it uses, or intends to use. The protective security assessment must review the findings and results of other protective security-related reports, such as the penetration testing report (see section 9.4) and address any findings or recommendations arising from the essential strategies review.

The assessor who prepares the protective security assessment must be external to the organisation and must not have been involved in the design, implementation, operation or management of the applicant's DI data environment or accredited services.

See rules 3.3–3.5 in the Accreditation Rules for the requirements relating to the protective security assessment.

Fraud assessment

The fraud assessment is a key mechanism for determining that the applicant has, or will, implement and operate an effective framework of fraud controls associated with its DI data environment and accredited services.

The assessor who prepares the fraud assessment must be external to the applicant and must not have been involved in the design, implementation, operation or management of the applicant's DI data environment or accredited services.

See rule 3.6 in the Accreditation Rules for the requirements relating to the fraud assessment.

Accessibility and useability assessment

The accessibility and useability assessment must review and assess the applicant's compliance with the accessibility and useability requirements of the Act and the Accreditation Rules, with the aim of ensuring that accredited services are accessible for individuals who experience barriers when creating or using a digital ID.

The assessment must review and assess the findings of the Web Content Accessibility Guidelines testing and address any risks or recommendations identified by the assessor.

See rule 3.7 in the Accreditation Rules for the requirements relating to the accessibility and useability assessment.

9.4 Systems testing

Penetration testing

Penetration testing is an assessment and evaluation of the effectiveness of security controls in the IT system through which the applicant provides, or will provide, its accredited services.

Penetration testing is intended to provide a level of confidence to the Regulator that the applicant's IT system does not include security vulnerabilities that could be exploited.

The assessor who prepares the penetration testing must be external to the organisation and must not have been involved in the design, implementation, operation or management of the applicant's DI data environment or accredited services.

See rules 3.8–3.10 in the Accreditation Rules for the requirements relating to penetration testing.

Useability testing

Useability testing is used to identify issues with user experience resulting from adverse issues in the design, useability and accessibility of the applicant's public-facing accredited services.

It also identifies to what degree those services can be accessed and used by a diverse range of people within the Australian community, covering diversity in disability, age, gender and ethnicity, and still operate as intended.

See rules 3.11–3.13 in the Accreditation Rules for the requirements relating to useability testing.

Web Content Accessibility Guidelines

An applicant must test that its public facing accredited services and information relating to its accredited services meet applicable Web Content Accessibility Guidelines.

See rules 3.14–3.16 in the Accreditation Rules for the requirements relating to Web Content Accessibility Guidelines testing.

10. Review of Regulator decisions

Certain decisions of the Regulator are reviewable. This includes decisions of the Regulator to accredit or not accredit an entity. Some reviewable decisions are eligible for internal review by the Regulator, while others are only eligible for external review by the Administrative Review Tribunal or Federal Court.

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

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

10.1 Internal review

A reviewable decision will be eligible for internal review if it is made by a delegate of the decision maker.

Information provided on whether the decision made by the Regulator is eligible for internal review will include contact information for submitting a request for 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 applicant. A request for review of a decision made by the Regulator must be made by the affected entity.

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 applicant 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 applicant 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 (ART) if the decision was made by the decision maker personally, or if the decision is an internal review decision of the reviewable decision made by the Regulator.

The Regulator will advise the applicant if the decision is eligible for external review by the ART. An application to the ART 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 Tribunal for a review of a decision is available on the ART website.

10.3 Judicial review

Applicants or accredited 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
- the decision maker took an irrelevant consideration into account or failed to take a relevant consideration into account
- 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 ART. 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 accreditation

11.1 Digital ID Accredited Entities Register

Upon notification by the Regulator that an application for accreditation has been successful, details of the accredited entity and accredited services will be placed on the Digital ID Accredited Entities Register, and the accredited entity can utilise the Digital ID Accreditation Trustmark for its accredited services.

- The Digital ID Accredited Entities Register contains details of Digital ID providers that are, or have been, accredited under the Act.
- The Digital ID Accredited Entities Register includes the type of accredited service each organisation is accredited to provide, the day the accreditation came into force, and any conditions that were imposed on accreditation.

The Digital ID Accredited Entities Register may also contain any other information the Regulator considers appropriate. The register is available on the:

- Digital ID System website
- ACCC Digital ID public register.

11.2 Digital ID Accreditation Trustmark

An accredited entity is entitled to use the Digital ID Accreditation Trustmark in accordance with the requirements prescribed in the Act and Digital ID Rules. The entity must also ensure that its use of the Digital ID Accreditation Trustmark complies with the Australian Consumer Law.

If an accredited entity chooses to use or display the Digital ID Accreditation Trustmark, it must:

- take reasonable steps to make clear which services are accredited and which are not
- use and display a hyperlink to the Digital ID Accredited Entities Register near the Digital ID Accreditation Trustmark
- use and display the internet address of the Digital ID Accredited Entities Register near the Digital ID Accreditation Trustmark (for printed documents).

If an accredited identity exchange provider chooses to use or display the Digital ID Accreditation Trustmark, it must ensure it is only used or displayed on:

- public-facing accredited services
- any document that contains public-facing information related to the accredited services of that identity exchange provider or another accredited entity operating within the same digital ID system.

Chapter 5 of the Digital ID Rules details the requirements in relation to the Digital ID Accreditation Trustmark.

11.3 Changes to conditions on accreditation

The Regulator may, on its own initiative, take action to impose new conditions, as well as vary or revoke an existing condition on an entity's accreditation, if it considers it appropriate to do so. The Regulator may also be directed by the Minister to impose new conditions on an entity's accredited service.

An accredited entity can also apply to the Regulator to have a new condition imposed on the entity's accreditation, or to have an existing condition varied, or revoked, using the *Conditions on Accreditation or AGDIS Approval form*. The accredited entity will need to provide details and justification for the condition(s) the entity is seeking to have imposed, varied or revoked. This form is available on the Digital ID System website. The form and accompanying evidence must be submitted to the Regulator.

11.4 Varying accreditation

The Regulator may vary an entity's accreditation to reflect a change to the accredited entity's name.

Applications for accreditation to be varied to reflect a change to the accredited entity's name can be made in writing to the Regulator via *the Application to vary Accreditation or AGDIS Approval form* available on the Digital ID system website. The form requires information about the accredited entity's new name and any relevant dates. This form must be submitted to the Regulator.

The Digital ID Accredited Entities Register will be updated following a decision by the Regulator to vary the accredited entity's name.

11.5 Suspending and revoking accreditation

An entity's accreditation can be suspended or revoked in 3 instances:

- by direction of the Minister for Finance
- on the Regulator's initiative
- by application from the entity.

The Minister can direct the Regulator to suspend or revoke an accreditation

The Regulator must suspend or revoke an entity's accreditation 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.

The Regulator may suspend or revoke an accreditation

The Regulator may, on its own initiative, suspend or revoke an entity's accreditation in some circumstances, including where the Regulator reasonably believes:

- the accredited entity has contravened or is contravening the Act
- there has been a cyber security incident involving the entity, or a cyber security incident involving the entity is imminent
- it is not appropriate for the entity to be accredited, for example by reference to the fit and proper person requirements in the Digital ID Rules.

An entity can apply to suspend or revoke its accreditation

An accredited entity may apply to the Regulator to have its accreditation suspended or revoked. The application must be made in writing using the *Suspension of Accreditation or AGDIS Approval form* or the *Revocation of Accreditation or AGDIS Approval form* available on the Digital ID system website.

The application requires information about the services that are to be suspended or revoked, the reason for the request and any relevant dates. The application must be submitted to the Regulator.

If an entity makes an application seeking suspension of its accreditation, the Regulator retains the discretion to approve or reject the entity's application. Once the Regulator has suspended the entity's accreditation, the suspension remains in force until the entity requests the suspension be revoked.

If a revocation of the entity's accreditation is sought, the Regulator must accept that application, but the Regulator can determine the date that the revocation takes effect.

The Digital ID Accredited Entities Register will be updated to reflect any decisions to suspend or revoke an entity's accreditation.

12. Compliance obligations

Following accreditation, entities have continuing compliance, disclosure and reporting obligations under the Digital ID legislation.

These obligations include:

- complying with conditions applied to the entity's accreditation
- complying with the requirements for maintaining accreditation as set out in Chapter 4 of the Accreditation Rules, including ensuring that the accredited entity's protective security and fraud management capabilities are adapted to respond to existing and emerging risks, threats and vulnerabilities
- complying with the requirements set out in Chapter 5 of the Accreditation Rules when providing accredited services
- ensuring that the accredited services an entity provides are accessible and inclusive as required by the Act
- complying with restrictions on the collection of restricted attributes of individuals (relevant to participating relying parties)
- notifying the Regulator of reportable incidents within required timeframes
- maintaining comprehensive records as required by the Accreditation Rules
- participating in annual review processes and ongoing reporting obligations as required by the Accreditation Rules.

In addition, an entity must ensure that any representation it makes regarding its accreditation or accredited services provided under the Act is accurate, and not misleading or deceptive.

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

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

- record keeping obligations
- reportable incident obligations
- annual review and reporting obligations.

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

12.1 Record keeping obligations

Accredited entities must comply with the record keeping requirements set out in the Accreditation Rules. For example, accredited entities must prepare and keep records related to:

- cyber security incidents that cause, or are likely to cause, serious harm to one or more individuals
- digital ID fraud incidents, and
- data breaches.

See rules 4.18, 4.35, 4.46 and 7.8 of the Accreditation Rules for the record keeping obligations.

Records must be kept for a minimum of 3 years from the day of generation and must not contain biometric information. Additional record keeping requirements apply if the information relates to any current or anticipated legal or dispute resolution proceedings, or a current compliance or enforcement investigation.

For accredited entities participating in the AGDIS, there are additional record keeping obligations under the Act and Digital ID Rules.

12.2 Reportable incident obligations

Accredited entities have obligations to report certain incidents to the Regulator. The obligations to notify reportable incidents vary depending on whether the accredited entities are providing their accredited services in:

- the AGDIS, or
- a digital ID system other than the AGDIS.

The following are examples of reportable incidents for accredited entities:

Notifications of reportable incidents

The accredited entity must notify the Regulator:

- of any material change that results in, or reasonably likely to result in:
  - a material or adverse impact on the entity's DI data environment, or
  - an adverse impact on the entity's ability to comply with its legal obligations
- of any matters that could reasonably be relevant to a decision as to whether the accredited entity, or an associated person of the entity, is a fit and proper person
- of any changes to, or error in, any of the information provided to the Regulator
- of any change in control under section 910B of the Corporations Act
- if the entity intends to cease providing its accredited services.

In addition, an accredited entity has obligations to provide the Regulator with a copy of any statement it gives to the OAIC in relation to eligible data breaches: see sections 38–40 of the Act.

For accredited entities participating in the AGDIS, there are additional notification obligations under the Act and Digital ID Rules.

Failure to comply with certain notification requirements may result in enforcement action, including proceedings seeking injunctions and/or substantial civil pecuniary penalties in appropriate cases.

See Chapter 3 of the Digital ID Act and Chapter 7 of the Accreditation Rules for obligations relating to reportable incidents. For accredited entities that participate in the AGDIS, see also Chapter 4 of the Digital ID Rules

12.3 Annual review and reporting

To maintain accreditation, accredited entities must conduct annual reviews and provide an annual report to the Regulator.

The annual review reporting periods for accredited entities vary depending on whether the entity is a transitioned entity under the *Digital ID (Transitional and Consequential Provisions) Act 2024* or an entity accredited by the Regulator under the Digital ID Act.

When submitting an annual report to the Regulator, accredited entities must also include an attestation statement, signed by the accredited entity's accountable executive, that attests to the content of the report. This includes that in the relevant reporting period the entity met all its annual review and reporting requirements, except for any non-compliance notified to the Regulator.

See Chapter 6 of the Accreditation Rules for more information about annual review requirements.

Appendix A – Assessor qualifications

The information below is intended to provide guidance on assessor qualifications. It is not intended to be exhaustive, and an applicant should satisfy itself that an assessor is appropriately qualified to conduct the relevant assessment.

Privacy impact assessment

When selecting assessors to undertake the required privacy impact assessment, applicants should consider using assessors that have qualifications in privacy law and have experience in practicing privacy law or privacy auditing. This can include assessors who are a Certified Information Privacy Professional under the International Association of Privacy Professionals. The privacy assessment must be conducted in consultation/coordination with the designated Privacy Officer of the applicant.

Fraud assessment

When selecting assessors to undertake the required fraud assessment, applicants could consider the following:

- Government entities could utilise assessors that have undertaken relevant training through the following bodies:
  - Commonwealth Fraud Prevention Centre
  - Australian Government Investigation Standards (AGIS)
- Private entities could utilise assessors that are qualified and have an understanding of the Australian Standard AS8001 Fraud and Corruption Controls.

Protective security assessment

Relevant assessor qualifications to consider include:

- If the applicant utilises ISO/IEC 27001, in order to complete their protective security assessment, the assessor conducting the assessment must be accredited, or recognised, by the Joint Accreditation System of Australia and New Zealand (JASANZ) to certify entities against ISO/IEC 27001.
- If the applicant utilises the PSPF framework or a different security framework / standard from the PSPF or ISO27001, they should ensure that the assessor meets the certification to conduct the assessment and be able to map the controls against those from either ISO or PSPF. The applicant also needs to ensure the evidence is sufficient to cover the requirements under the Accreditation Rules.

- It is also recommended that the assessor be endorsed under the Australian Signals Directorate, Infosec Registered Assessors Program (IRAP), or have obtained the auditing qualification of an Infosec Registered Assessors Program. This could include but is not limited to:
  - Certified Information Systems Auditor
  - Certification in Risk and Information Systems
  - GIAC Systems and Network Auditor certification
  - ISO 27001 Lead Auditor
  - PCI Qualified Security Assessor.

Penetration testing

The assessor for penetration testing could have qualifications relevant to Penetration Testing levels 4 or 5 outlined by the SFIA Foundation. The CREST (Council of Registered Ethical Security Testers) can provide the information regarding Penetration Testing certification.

Useability testing

The assessors for useability testing could have qualifications that meets the User level of 4 or higher under SFIA online User research URCH. https://sfia-online.org/en/sfia-8/skills/user-research.

Web Content Accessibility Guidelines testing

Assessors used to undertake Web Content Accessibility Guidelines testing may be members of, or certified under, associations or organisations such as the World Wide Web Consortium (W3C) or the International Association of Accessibility Professionals (IAAP).

Appendix B – Evidence listed in the accreditation application form

General Information – please note these documents are mandatory

- Statement of scope and applicability
- Description of the DI Data Environment
- Evidence of technical testing (such as in the form of a requirements traceability matrix – see information under "technical testing" in section 8.4)
- Technical testing attestation statement
- Diagram showing corporate ownership (including percentages held by each owner).

Conditions

- Supporting evidence for any conditions sought by the applicant (if applicable).

Evidence it is appropriate to accredit the organisation

- Evidence it is appropriate to accredit or approve the organisation form.

Privacy

- Privacy impact assessment [mandatory]
- Organisation's response to privacy impact assessment [mandatory]
- Privacy management plan(s)
- Privacy policy(s)
- Data breach response plan(s)
- Any other document supporting the applicant's ability to comply with privacy requirements.

Fraud

- Fraud assessment [mandatory]
- Organisation's response to fraud assessment [mandatory]
- Fraud risk assessment [mandatory]

- Fraud control plan
- Fraud incident detection, investigation, response and reporting procedures
- Any other document supporting the applicant's ability to comply with fraud requirements.

Protective Security

- Protective security assessment [mandatory]
- Organisation's response to protective security assessment [mandatory]
- Cyber security risk assessment [mandatory]
- System security plan
- Cloud services management plan (if applicable)
- Cloud services providers register (if applicable)
- Penetration testing report [mandatory]
- Essential strategies review report
- Protective security incident detection, investigation, response and reporting procedures
- Disaster recovery and business continuity plan
- Logging implementation and monitoring plan
- Any other document supporting the applicant's ability to comply with protective security requirements.

Accessibility and Useability

- Accessibility and useability assessment [mandatory]
- Organisation's response to accessibility and useability assessment [mandatory]
- Useability testing report
- Web Content Accessibility Guidelines testing report
- Any other document supporting the applicant's ability to comply with accessibility and useability requirements.

Role specific requirements

Biometrics

- Biometric binding processes documentation
- Test plan and processes (as required)
- Ethical policies and procedures (as required)
- Presentation attack detection technology testing report [mandatory]
- Identity service provider's response to presentation attack detection technology testing report (as required)

- Biometric matching algorithm testing report
- Evidence of source biometric matching testing
- eIDVT testing report
- Any other document supporting the applicant's ability to comply with biometrics requirements.

Identity proofing

- Identity proofing process
- Event logging implementation and monitoring plan
- Risk assessment for use of alternative proofing process (if applicable)
- Any other document supporting the applicant's ability to comply with identity proofing requirements
- Alternative proofing proposal and processes (if applicable).

Authentication management

- Cryptographic key management processes and procedures
- Any other document supporting the applicant's ability to comply with authentication requirements.

Accredited identity service providers

- System design
- Any other document supporting the applicant's ability to comply with the identity service provider requirements.

Accredited identity exchange providers

- Digital ID system rules (for private organisations only who provide services in a system that includes non-accredited services)
- System design [mandatory]
- Any other document supporting the applicant's ability to comply with identity exchange provider requirements.


AUSTRALIA


ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION