AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Guidance for accredited entities in Australia's Digital ID Sytem

Version 1

June 2025

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

ACCC 06/25_25-27

www.accc.gov.au

Contents

1. Introduction

The purpose of this guidance is to assist accredited entities in Australia's Digital ID System in understanding their ongoing obligations under the Digital ID legislation and the processes when applying for or notifying the Australian Competition and Consumer Commission (ACCC) of changes to their accreditation.

The guidance also explains the ACCC's approach to promoting compliance with the Digital ID legislation, and the ACCC's powers as the Digital ID Regulator.

The ACCC may update this guidance periodically and entities should visit the Digital ID System website to ensure they are reading the latest version.

Organisations that are interested in applying to become accredited, or that are seeking more information about the application requirements, should refer to *Applying for accreditation – Guidance for organisations seeking to become accredited in Australia's Digital ID System*.

Accredited entities that are also participating in the Australian Government Digital ID System (AGDIS) should refer to *Guidance for entities approved to participate in the Australian Government Digital ID System* for information about the ongoing obligations of AGDIS participants.

These guidance documents are available on the Digital ID System website.

The ACCC's guidance does not replace the requirement for applicants and accredited entities to have a full understanding of the Digital ID legislation. Entities should seek their own professional advice about the Digital ID legislation.

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

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 Australian Government Digital ID System (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)	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)	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)	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*	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)	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 Digital ID legislation. 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 mean 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 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 in respect of the privacy aspects of the Digital ID 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 Digital ID Act.

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

Office of the System Administrator

The Office of the System Administrator (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.

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.

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

Accredited entities and applicants can contact the Regulator via email at DigitalIDRegulator@accc.gov.au.

Where this guidance lists requirements to provide information to or contact the Regulator, this is to be done via the above email address.

Submitting forms and supporting evidence

This guidance sets out the names of forms associated with certain requests, which are available on the Digital ID System website. Importantly, all forms must be submitted by a person who is authorised to act on behalf of the entity.

Where there are forms or supporting evidence associated with requests or notifications to the Regulator, these documents should be provided via a secure link provided by the Regulator.

Entities that received a secure link during the application stage can continue to use that link. Entities that do not have a link or require it to be re-sent, can email the Regulator via the above email address to request a link.

4. Requirements for maintaining accreditation

Following accreditation, entities have on-going compliance, disclosure and reporting obligations under the Digital ID legislation. It is the responsibility of each accredited entity to be aware of and comply with its legal obligations under the Digital ID legislation, including the Act and all rules and standards.

This chapter summarises some of the key obligations of accredited entities. However, it is not a comprehensive or exhaustive list of all obligations accredited entities must comply with, and accredited entities should seek their own professional advice about their legal obligations under the Digital ID legislation.

Rule 1.8 of the Accreditation Rules lists specific rules which do not apply to transitioned entities for the first 12 months from the commencement of the Accreditation rules.

Accredited entities' obligations include:

- maintaining the boundaries of the entity's digital ID (DI) data environment and the entity's statement of scope and applicability
- complying with privacy obligations imposed by the Digital ID legislation and any other relevant legislation
- taking reasonable steps to continuously improve protective security and fraud management capabilities
- taking reasonable steps to ensure that the accredited services an entity provides are accessible and inclusive
- complying with the requirements set out in the Accreditation Rules for the collection, retention, use, disclosure and destruction of biometric information
- complying with conditions applied to the entity's accreditation
- ensuring that the Digital ID Accreditation Trustmark is used in accordance with the Act, the Digital ID Rules and the Trade Mark Licence Agreement
- notifying the Regulator of reportable incidents within required timeframes, including any material changes or any matter that could reasonably be considered relevant to a decision as to whether the entity is a fit and proper person
- complying with the requirements for maintaining accreditation as set out in Chapter 4 of the Accreditation Rules, which include:
  - ensuring the entity's protective security and fraud management capabilities are allocated adequate budget and resources
  - providing for management oversight of the entity's protective security and fraud management capabilities
  - ensuring the entity's protective security and fraud management capabilities are appropriate and adapted to respond to cyber security and fraud risks
  - maintaining appropriate mechanisms for cyber security and fraud incident detection, investigation, response and reporting
  - complying with the privacy rules under Part 4.3

- maintaining and complying with a data breach response plan
- maintaining comprehensive records and meeting logging requirements, including through a logging implementation and monitoring plan

- complying with requirements for providers detailed in Chapter 5 of the Accreditation Rules. This includes requirements relating to the generation and management of digital IDs and attributes of individuals within a digital ID system.

As well as the ongoing obligations discussed in this chapter, accredited entities are required to complete an annual review, comprising of an annual report which includes an attestation statement signed by the accountable executive of the accredited entity. More information about annual reviews and reporting periods for entities are detailed in section 5.

Failure to meet compliance obligations may result in enforcement action by the Regulator, including suspension or revocation of accreditation and civil penalty proceedings seeking injunctions and/or substantial pecuniary penalties.

4.1 DI data environment and statement of scope and applicability

Digital ID (DI) data environment

DI data environment refers to the IT systems used for, and the processes that relate to, the provision of an entity's accredited services. When applying for accreditation, an entity will have included a document detailing its DI data environment to the Regulator.

An accredited entity must, at least once in each reporting period, review the boundaries of its DI data environment and update the documented boundaries to ensure it has correctly and completely defined and documented the boundaries at the time of the review. The Regulator may also ask for an updated version of the DI data environment at the time of reviewing an application for variation of a condition on accreditation, or in response to a material change notification (see section 4.10).

A well-defined DI data environment is critical to:

- understanding when and how an entity's accredited services collect, hold, use or disclose personal information as defined by the Act
- determining which rules apply to an entity's accredited services
- implementing appropriate controls to mitigate risks associated with an entity's accredited services.

Limiting the boundaries of a DI data environment to the extent practicable is particularly important where an accredited entity uses the same infrastructure, IT systems and/or contractors, in whole or in part, for both its accredited and unaccredited services.

Statement of scope and applicability

A statement of scope and applicability lists each requirement in the Accreditation Rules and the Accreditation Data Standards that an entity must comply with in relation to its accredited

services. For accredited entities, it lists the evidence to demonstrate that an entity complies with those requirements.

An entity will have provided a statement of scope and applicability to the Regulator when applying for accreditation.

An accredited entity must, at least once in each reporting period, review its statement of scope and applicability for completeness and accuracy. An accredited entity must also review its statement of scope and applicability for completeness and accuracy when it becomes aware of a material change to the extent and nature of threats to its DI data environment.

The Regulator may also ask for an updated statement of scope and applicability at the time of reviewing an application to impose, vary or revoke a condition on accreditation, or in response to a material change notification (see section 4.10).

Part 4.6 of the Accreditation Rules details the requirements relating to an entity's review of its DI data environment and statement of scope and applicability.

Rule 2.1 of the Accreditation Rules contains more information about defining an entity's DI data environment.

4.2 Privacy

The Act imposes several additional privacy safeguards on accredited entities to strengthen requirements for how personal information and digital ID data is handled. These privacy obligations operate in addition to the general obligations under either the *Privacy Act 1988* (Cth) or relevant state or territory privacy legislation.

The OAIC, as the privacy regulator for Digital ID has developed detailed guidance for accredited entities. This is available at: Privacy materials for accredited entities.

The privacy obligations for accredited entities under the Digital ID legislation include:

- only collecting personal information that is reasonably necessary for an entity to provide an accredited service
- requirements to obtain express consent before sharing personal information or restricted attributes with relying parties (entities that rely on an attribute of an individual provided by an accredited entity to provide or facilitate an individual's access to a service)
- prohibitions on the collection of certain information about individuals, such as racial or ethnic origin, religious beliefs and political opinions
- prohibitions on data profiling and the use of personal information for marketing purposes
- restrictions on the collection, use, disclosure and retention of biometric information, including a prohibition on one-to-many matching
- having a privacy policy that provides sufficient detail for an individual to understand how their personal information is collected, used and disclosed
- requirements to have, maintain and comply with a data breach response plan, and notify the OAIC and the Regulator in the case of a data breach in accordance with the legal requirements to which an entity is subject.

The Accreditation Rules also require an accredited entity that is not a government agency for the purposes of the *Privacy Act 1988* (Cth) to comply with the *Privacy (Australian Government Agencies*

— *Governance) APP Code 2017* (privacy governance code) in respect of its accredited services and DI data environment.

The privacy governance code requires agencies to have, among other things, a privacy officer, privacy champion, privacy management plan, register of privacy impact assessments, privacy education and training.

Agencies are also required to conduct a privacy impact assessment for all high privacy risk projects (which may include a change to conditions) and regularly review their internal privacy processes.

See Chapter 3 of the Act and Part 4.3 of the Accreditation Rules for more information about an entity's privacy obligations.

4.3 Protective security

The Accreditation Rules require accredited entities to have and maintain a protective security capability to effectively manage the security of their DI data environment.

An entity's protective security capability means its ability to manage the protective security of its DI data environment through its implementation and operation of processes and controls.

An entity must allocate adequate budget and resources and provide for management oversight to ensure the effective operation of controls to manage cyber security risks. An accredited entity's protective security capability must be appropriate and adapted to respond to cyber security risks, including any emerging risks.

An accredited entity must take reasonable steps to prevent, detect and deal with cyber security incidents by having, maintaining and continuously improving its protective security capability, and implementing and maintaining appropriate monitoring and detection mechanisms.

See Rule 1.5 of the Accreditation Rules for the meaning of taking reasonable steps.

The Accreditation Rules also impose obligations on entities to implement and comply with protective security frameworks. An entity's continuous compliance with a protective security framework such as ISO/IEC 27001, PSPF, or an alternative framework, supports the prevention, detection and management of cyber security incidents.

The Accreditation Rules prescribe additional protective security controls that accredited entities must comply with. These include:

- conducting a cyber security risk assessment for each reporting period associated with their accredited services and DI data environment
- having, maintaining and complying with a System Security Plan
- implementing and complying with 'Essential Eight' cyber security strategies
- implementing and maintaining appropriate mechanisms for preventing, detecting and reporting actual and suspected cyber security incidents and alerting an entity's personnel to such incidents
- implementing and maintaining mechanisms for investigating and dealing with cyber security incidents which relate to an accredited entity's DI data environment

- having, maintaining and complying with a separate disaster recovery and business continuity plan for their DI data environment
- maintaining logs to capture various activities, exceptions, faults and events in the entity's DI data environment, for example, the destruction of personal and biometric information, changes in access privileges, system alerts related to cyber security risks and unauthorised access attempts
- having, maintaining and complying with a logging implementation and monitoring plan that outlines how logs are generated, stored, protected, monitored and analysed to identify any anomalous behaviour
- developing, implementing and maintaining documented, effective and secure processes and procedures for managing cryptographic keys relevant to an entity's IT system
- having and maintaining, where applicable, a cloud services management plan and a register of cloud service providers used by an entity
- ensuring that all personal information collected, used, held or disclosed by or on behalf of the accredited entity is protected in transit and at rest by approved cryptography
- considering the implications of their decisions relating to cyber security risks and sharing information about known cyber security risks or incidents with other impacted participants of the digital ID system(s) in which they operate, as appropriate
- taking reasonable steps to ensure the ongoing eligibility and suitability of their personnel who interact with the DI data environment.

The Accreditation Rules also require identity service providers to provide advice to individuals about how to safeguard their digital ID against cyber security risks and update that advice, as soon as practicable, as new risks and threats emerge. An accredited entity providing public-facing accredited services must provide support services to individuals who have been adversely affected by a cyber security incident.

See Chapter 4 of the Accreditation Rules for more information about the requirements for maintaining accreditation, including protective security controls (Part 4.1).

4.4 Fraud

The Accreditation Rules contain fraud control requirements for accredited entities.

An accredited entity's fraud management capability refers to its ability to manage fraud in relation to its accredited services and DI data environment through the implementation and operation of processes and controls. This includes by allocating adequate budget and resources and providing for management oversight.

An accredited entity must take reasonable steps to prevent, detect and address digital ID fraud incidents, including by maintaining and continually improving a fraud management capability that can adapt and respond to emerging fraud risks.

The Accreditation Rules prescribe the requirements for accredited entities to implement fraud controls, including, but not limited to:

- appointing a fraud controller for managing fraud risks and facilitating an entity's compliance with fraud control requirements
- for each reporting period, conducting a fraud risk assessment associated with an entity's accredited services and DI data environment

- having, maintaining and complying with a fraud control plan
- implementing and maintaining appropriate mechanisms for preventing, detecting and reporting digital ID fraud incidents
- implementing and maintaining mechanisms for investigating and responding to digital ID fraud incidents
- sharing information about fraud risks with other participants of the digital ID system(s) in which they operate, as appropriate
- providing appropriate training to educate relevant personnel about fraud risks, fraud concepts and individual responsibilities relating to an accredited entity's management of Digital ID fraud incidents, before personnel start work and at least once every 12 months after.

The Rules also require accredited entities to provide advice to individuals about how to safeguard their digital ID against digital ID fraud risks and update that advice, as soon as practicable, as new risks and threats emerge. An accredited entity providing public-facing accredited services must also provide support services to individuals who have been adversely affected by a digital ID fraud incident.

See Chapter 4 of the Accreditation Rules for more information about the requirements for maintaining accreditation, including fraud controls (Part 4.2).

4.5 Accessibility and inclusivity

The accredited services an entity provides must be accessible for individuals who experience barriers when creating or using a digital ID.

The accessibility and useability requirements contained in the Accreditation Rules require accredited entities to:

- provide individuals with a clear and simple description of the entity's accredited services
- present public-facing information related to their accredited services in a clear and simple manner, using plain language
- take reasonable steps to ensure public-facing information related to accredited services is in multiple accessible formats
- provide assisted digital support to individuals who may experience barriers when creating or using a digital ID (for example, a monitored email address, chat function or phone support) and publish details of such support
- comply with accessibility standards and consider accessibility guidelines specified in the Accreditation Rules
- have written processes and procedures that allow individuals to seek assistance or otherwise resolve disputes or complaints in relation to the entity's public-facing accredited services
- obtain and record feedback about the useability and accessibility of the entity's public-facing accredited services.

In addition, every reporting period, an accredited entity must prepare a report detailing any reasonable steps it has taken during the reporting period to ensure its accredited services are accessible for individuals who experience barriers when creating or using a digital ID. An entity must also detail

any reasonable steps it proposes to take in the next reporting period to improve the accessibility of its services.

The Rules also prescribe the accessibility and useability requirements that an identity service provider must comply with in relation to identity proofing processes.

Section 30 of the Digital ID Act requires accredited services to be accessible and inclusive.

See Chapter 4, Part 4.4 in the Accreditation Rules for accessibility and inclusivity requirements.

See Chapter 5, Division 4 of Part 5.1 in the Accreditation Rules for accessibility and useability requirements for accredited identity service providers when providing accredited services.

4.6 Biometric information

Accredited entities that collect, use, retain, and disclose biometric information are subject to legislative obligations and additional privacy safeguards in the Act. These include:

- restrictions and limitations such as prohibition of one-to-many matching
- limiting retention to no longer than 14 days to conduct testing or fraud investigation
- obtaining express consent from the individual that the information relates to when using biometric information for authentication and verification purposes
- taking reasonable steps to continuously improve biometric technology systems to ensure they do not selectively disadvantage or discriminate against any group
- obligations to destroy biometric information and to log records of this destruction.

For more information on obligations relating to biometric information, entities should refer to the OAIC's privacy guidance for accredited entities. This includes information about permissible limited disclosure for law enforcement purposes, handling and destruction of biometric information, and requirements for confirming an individual's express consent (including the process for withdrawing consent).

See Chapter 3, Division 2 of the Act for the additional privacy safeguards.

Biometric testing

For accredited entities authorised to retain, use, or disclose biometric information to verify an individual and undertake testing using biometric information, the Act requires these entities to take reasonable steps to ensure their biometric systems do not selectively disadvantage or discriminate against any group.

See Section 49A of the Act for the requirements relating to biometric testing and continuous improvement.

Importantly, an accredited entity must ensure that any testing using biometric information is conducted in accordance with the Accreditation Rules on the use of biometric information in testing. These rules are intended to limit the use and retention of biometric information to specific purposes that improve an entity's accredited services for the benefit of users.

Accredited entities may not use and retain biometric information of individuals for testing that is outside of the purposes listed in the Accreditation Rules.

Testing must be undertaken in accordance with a testing plan that includes information such as the purpose, objectives and methodology of the testing and how biometric information will be stored and protected during the testing.

The testing must be conducted in accordance with the accredited entity's system security plan and with one or more policies covering the ethical use of biometric information. Personnel conducting biometric testing must be appropriately qualified and have the requisite skills and experience in conducting biometric testing.

An accredited entity must confirm how the biometric information will be destroyed at the end of testing, or within a period of no longer than 14 days, as specified in the Act. Once every reporting period, an accredited entity must prepare a report detailing the results of any testing using biometric information.

See rule 4.50 in the Accreditation Rules for the requirements relating to biometric information used for testing activities.

External biometric testing

Accredited entities that plan to apply for a condition to use biometric information of individuals for identity verification and/or authentication purposes, must undertake external biometric testing. This testing must be conducted by a biometric testing provider that is certified to assess biometric technology testing standards listed in the Accreditation Data Standards.

The testing that is required depends on whether an entity offers biometric capabilities related to authentication or verification for identity proofing.

Biometric testing will be required for the following online biometric binding methods and their biometric matching algorithms and techniques:

- technical biometric matching
- source biometric matching
- electronic identity verification technology (eIDVT) matching (only for identity proofing at level IP2 Plus)
- testing of a custom biometric capability for authentication in accordance with Accreditation Data standard 3.13.

Each entity that conducts online biometric binding or authentication using biometric information with a custom biometric capability must also undergo external testing for presentation attack detection.

See Chapter 2, Part 1 in the Accreditation Data Standards for the biometric testing requirements.

See Chapter 2, Part 2, Division 5 in the Accreditation Data Standards for testing authentication using biometric information requirements.

See Part 5.1, Division 2, subdivision B in the Accreditation Rules for the requirements relating to verification using biometric information.

4.7 Conditions

Accredited entities must comply with all conditions imposed on their accreditation.

Some conditions are imposed by default by the Act and the Accreditation Rules. For example, a default condition that applies broadly is simply that accredited entities must comply with the Act (see section 17 of the Act).

Conditions can also be imposed by the Regulator, either on its own initiative or on application by the entity. The Minister for Finance may also direct the Regulator to impose a condition on an entity's accreditation.

Common conditions

Another set of conditions that accredited entities may need to comply with are those specified in rule 7.3 of the Accreditation Rules, which are common conditions imposing limitations on the collection and disclosure of restricted attributes and the biometric information of individuals. The application of these conditions will vary depending on the kind of accredited services being provided and an entity's circumstances.

If an entity relies on one or more of the common conditions specified in rule 7.3 when providing its services, it must also comply with other relevant requirements in the Digital ID legislation, and the Regulator may require the entity to provide evidence to demonstrate compliance.

If an entity starts relying on a common condition after its accreditation has been granted this will likely constitute a material change and the requirement to notify the Regulator applies (see section 4.10). It is also recommended that an entity notify the Regulator in advance of its intention to rely on a common condition.

Accredited entities approved to participate in the AGDIS

Accredited entities participating in the AGDIS that have separate conditions imposed on their accreditation and approval must comply with all conditions.

Failure to comply with a condition may result in the suspension or revocation of an entity's accreditation or approval to participate in the AGDIS.

Sections 16–23 of the Act and Part 7.2 of the Accreditation Rules detail the requirements in relation to conditions on accreditation.

4.8 Digital ID Accreditation Trustmark and trade mark

Accredited entities are permitted to use the Digital ID Accreditation Trustmark. The trustmark is also a registered trade mark in Australia.

An accredited entity that is not a Commonwealth entity must enter into a Trade Mark Licence Agreement with the ACCC before using the Digital ID Accreditation Trustmark.

The Trade Mark Licence Agreement sets out the legal rights and obligations of an accredited entity wishing to use or display the Digital ID Accrediation Trustmark, including the need to use it in accordance with the Accreditation Trustmark Style Guide. Copies of the Trade Mark Licence Agreement and the Accreditation Trustmark Style Guide are available on the Digital ID System website.

An accredited Commonwealth entity must agree to comply with ACCC conditions relevant to the use of the trustmark that will be advised to them at the time of accreditation.

All accredited entities must also ensure that any use of the Digital ID Accreditation Trustmark complies with the requirements prescribed in the Digital ID legislation and the Australian Consumer Law.

Specifically, under the Digital ID Rules an accredited entity using or displaying the Digital ID Accreditation Trustmark must:

- take reasonable steps to make clear which services provided by the entity are accredited and which are not;
- use and display a hyperlink to the Digital ID Accredited Entities Register near the Digital ID Accreditation Trustmark; and
- 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, the trustmark must only be used or displayed on:

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

Failure to comply with the provisions relating to the use or display of the Digital ID Accreditation Trustmark may give rise to substantial civil pecuniary penalties under the Act.

The Australian Consumer Law prohibits conduct in trade or commerce that is misleading or deceptive, or is likely to mislead or deceive, as well as false or misleading representations. Contraventions of the Australian Consumer Law may result in substantial civil pecuniary penalties.

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

4.9 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
- data breaches.

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

Record keeping refers to maintaining detailed and accurate records of relevant activities and events. This includes decisions to use civil, administrative, or disciplinary procedures, or to take no further action, in response to a cyber security incident, digital ID fraud incident or data breach. Record keeping allows transparency and accountability over how accredited entities handle such incidents.

These records are crucial documentation for analysis, audit trails, and improving incident response processes.

Under the Accreditation Rules, certain records must be kept for a minimum of 3 years from the day they were generated and must not contain biometric information. Additional record keeping requirements apply for the destruction or de-identification of certain personal information that relates to any current or anticipated legal or dispute resolution proceedings, or any current compliance or enforcement investigations under the Act.

When destroying or de-identifying personal information, entities also need to comply with privacy obligations under the *Privacy Act 1988* or applicable state or territory privacy laws.

In each reporting period, accredited entities are required to report on cyber security incidents and digital ID fraud incidents.

For accredited entities participating in the AGDIS, there are additional record keeping obligations under the Digital ID legislation. Accredited entities participating in the AGDIS must comply with all applicable record keeping obligations.

Failure to comply with record keeping requirements may give rise to substantial civil pecuniary penalties under the Act.

4.10 Notification obligations

Accredited entities are required to notify certain incidents to the Regulator within strict timeframes.

Under the Accreditation Rules, accredited entities must notify the Regulator of the reportable incidents in the table below within the corresponding timeframes.

An accredited entity must notify the Regulator:	
▪ of any material change	Within 5 business days.
▪ of any matter that could reasonably be relevant to whether the accredited entity, or an associated person of the accredited entity, is a fit and proper person	Within 5 business days.
▪ of any change to, or error in, any of the information the accredited entity has provided to the Regulator	Within 5 business days.
▪ of any change in control of the accredited entity under section 910B of the *Corporations Act 2001* (Cth)	Within 72 hours of the entity becoming aware or the change in control occurring.
▪ if the entity intends to cease providing its accredited services.	As soon as practicable after forming the intent.

To notify the Regulator of a reportable incident, entities must email the Regulator directly at DigitalIDRegulator@accc.gov.au. Entities should state the type of incident and the fact that it is a mandatory report in the email subject line.

In addition, accredited entities must provide the Regulator with a copy of any statement it gives to the OAIC or another entity, as required under the *Privacy Act 1988* or a law of the state or territory (notified entity), in relation to eligible data breaches or corresponding data breaches at the same time as the statement is given to the OAIC or notified entity (see sections 39–41 of the Act).

Accredited entities participating in the AGDIS are subject to additional notification obligations to the Regulator and the System Administrator under the Digital ID Rules.

See Part 7.3 of the Accreditation Rules for obligations relating to reportable incidents.

For accredited entities that participate in the AGDIS, see also Division 5 of Chapter 4 of the Act and Chapter 4 of Digital ID Rules.

Material change

Accredited entities are required to notify the Regulator within 5 business days of any material change.

A material change is defined in the Accreditation Rules as a change that alone or cumulatively results in, or is reasonably likely to result in, a material or adverse impact on an entity's proposed accredited services, accredited services or DI data environment. It could also be a change that has an adverse impact on an entity's ability to comply with the Act, the Accreditation Rules or the Accreditation Data Standards.

A material change is one that is real and quantifiable. It may consist, for example, of a series of small changes to an entity's processes for managing digital ID fraud incidents that cumulatively are considered material, or it may be a one-off change such as use of a new fraud detection system for accredited services.

When an accredited entity becomes aware of a material change, it must review its statement of scope and applicability for completeness and accuracy.

During the reporting period, an accredited entity may also need to conduct assurance assessments, systems testing, technical testing and/or biometric testing to assess or test the effect of the material change and to demonstrate that it continues to be able to comply with the Digital ID legislation. A full assurance assessment or system testing is not required if the material change does not affect all controls. The assessment or testing can be limited to those controls that may be affected.

If a material change is a high privacy risk project, the accredited entity is required to conduct a privacy impact assessment before making the change. Further information on this can be found in the OAIC's Guide to undertaking privacy impact assessments.

Fit and proper person

Accredited entities are required to notify the Regulator within 5 business days of any matter that could be relevant to whether the entity is a fit and proper person. Importantly, this obligation applies even if the entity was not required to 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 remain accredited. In deciding this, the Regulator may have regard to whether the entity is a fit and proper person.

Rule 7.4(b) in the Accreditation Rules contains the reportable incident requirement to notify the Regulator of matters relating to whether an entity is a fit and proper person.

See Chapter 2 of the Digital ID Rules for fit and proper person considerations.

5. Annual reviews

Accredited entities are required to conduct annual reviews to maintain their accreditation. The purpose of an annual review is to ensure that the Regulator can be satisfied that the accredited entity continues to meet its obligations under the Digital ID legislation.

An annual review requires an entity to:

- review any changes to its accredited services and DI data environment over the relevant reporting period and assess whether those changes have impacted an entity's compliance, or ability to comply, with the Digital ID legislation
- conduct required testing and/or assurance assessments (discussed below)
- review certain plans and ensure that they are appropriate and adapted to respond to risks and threats
- produce an annual report that contains all the information required by the Accreditation Rules.

Additionally, the entity's accountable executive will be required to sign an attestation statement, which includes attesting that the entity has complied with the Digital ID legislation during the relevant reporting period, except for any non-compliance the entity has notified to the Regulator.

The annual report and associated documentation should be submitted to the Regulator via a secure link (see section 3).

Reporting periods

An accredited entity's reporting period is the 12-month period for which the accredited entity is required to conduct its annual review. The specific dates of the reporting period will be unique to each accredited entity and will be determined by whether an entity transitioned to the legislated Digital ID system at the commencement of the Act, or otherwise by the date that an entity's accreditation was granted.

Assessments and tests that are required to be undertaken during a reporting period must be conducted as close as practicable to the end of the relevant reporting period.

5.1 Scope of annual review

Review of changes

As part of its annual review, an accredited entity must identify any changes to its accredited services and DI data environment that may affect its ability to comply with its obligations.

With every change identified for a reporting period, the entity must:

- consider the impact of the change on its accredited service and DI data environment
- consider whether the change, or all the changes together, may affect its ability to comply with the Digital ID legislation, including the Accreditation Rules and the Accreditation Data Standards
- assess whether the change is a material change (see section 4.10 for information on what constitutes a material change)
- update its statement of scope and applicability to address each material change identified

- provide the updated statement of scope and applicability to the assessor who conducts the relevant assurance assessments and systems testing.

An accredited entity that has had a condition imposed by the Regulator relating to the collection and disclosure of restricted attributes must also, for each reporting period, review whether the condition remains necessary.

Response to material changes

If an entity identifies a material change, it must:

- conduct assurance assessments or systems testing to the extent required to assess or test the effect of the material change, and to ensure and demonstrate that the entity can continue to comply with the controls and requirements of the Digital ID legislation (as discussed in further detail below)
- conduct technical testing to the extent that the material change relates to the functionality requirements outlined in rule 2.5(2) and 2.5(3) of the Accreditation Rules
- if the entity is an identity service provider that conducts biometric binding or authentication using biometric information, conduct testing of the presentation attack detection technology, the biometric matching algorithm, source biometric matching or the eIDVT for the activities affected by the material change.

Importantly, a full assurance assessment or system testing is not required if the material change does not affect all controls. In these circumstances, the assurance assessment or system testing may be limited to the controls that have been or may be affected by the material change.

If a material change is a high privacy risk project, the entity must conduct a privacy impact assessment prior to making the change (see rule 4.37 of the Accreditation Rules).

Review of plans

An entity must review each of its relevant plans (detailed below) to ensure they are appropriate and adapted to respond to risks and threats, including emerging risks and threats, to the entity's accredited services and DI data environment. The entity's accountable executive will be required to attest that this has been done as part of the annual report (see section 5.2).

The plans that an entity must review include its:

- system security plan
- fraud control plan
- disaster recovery and business continuity plan
- privacy policy
- privacy management plan
- data breach response plan.

Regular assessments and testing

All accredited entities are required to conduct regular assurance assessments, systems testing and technical testing. However, as described above, the frequency and scope of the assessments and testing will be determined by any material changes identified by the entity during the reporting period. The required frequency for undertaking the assessments and testing is set out in Table 1 below.

In addition to assessing or testing the effect of any material change, an entity must for the purposes of its annual review:

- conduct a fraud assessment and a protective security assessment for the annual review after the entity's first reporting period, and thereafter in every alternate reporting period (or more frequently if required to do so because of a material change)
- conduct penetration testing in each reporting period.

External assessors

The following assessments and tests must be undertaken by an external assessor (discussed in further detail below):

- fraud assessments (unless the criteria in rule 6.4 (2) of the Accreditation Rules are satisfied) (see rule 6.4)
- protective security assessments (see rule 3.3(2) of the Accreditation Rules)
- privacy impact assessment (see rule 2.4 of the Accreditation Rules)
- penetration testing (see rule 3.9 of the Accreditation Rules)
- presentation attack detection testing (see rule 6.5 of the Accreditation Rules).

Table 1: Assessment and testing requirements in the Accreditation Rules

Requirement	Additional assessor requirement	Required frequency for review
Protective security assessment (rule 3.3)	Yes, see rule 3.3(2) and (3)	Generally, every 2 years (see rule 6.4(3)) OR As per material change requirements in rule 6.3
Fraud assessment (rule 3.6)	Yes, see rule 3.6(2)	Generally, every 2 years (see rule 6.4(1) and other considerations column) OR As per material change requirements in rule 6.3
Accessibility and useability assessment (rule 3.7)	No	As per material change requirements in rule 6.3
Privacy impact assessment (rule 2.4)	Yes, see rule 2.4(2)	As per material change requirements in rule 6.3
Penetration testing (rules 3.8, 3.9 and 3.10)	Yes, see rule 3.9	Generally, every year (see rule 6.5(1))
Useability testing (rules 3.11, 3.12 and 3.13)	No	As per material change requirements in rule 6.3
Web Content Accessibility Guidelines testing (rules 3.14, 3.15 and 3.16)	No	As per material change requirements in rule 6.3
Presentation attack detection testing for identity service providers that conduct online biometric binding or authentication only (rule 6.5(2) (See section 2.3 of the Accreditation Data Standards for the requirements relating to presentation attack detection)	Yes	Generally, every 2 years (see rule 6.5(2)) OR As per material change requirements in rule 6.3
Technical testing (rules 2.5(2) and 2.5(3))	No	As per material change requirements in rule 6.3

Requirements for assurance assessments and systems testing

Assessor's report

Each time an assessor undertakes an assurance assessment or systems test as part of an entity's annual review, the assessor must prepare a report that meets the requirements of the Accreditation Rules (see rule 3.17), including but not limited to:

- details of the testing such as a summary of activities undertaken, the dates on which testing was commenced and completed, the release number or version number of the information technology system assessed, and version number of any document considered
- details of the evaluation or test methodology used
- the assessment findings, including details of any relevant non-compliance with the Digital ID legislation, risks identified and recommendations to treat the risks or to ensure compliance
- the qualifications and experience of the assessor.

Entity's response

An entity 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 identified risk that requires treatment in the assessor's report, as well as respond to each recommendation in the report
- detail the action it will take to address the risk or recommendation, the timeframe in which it will complete the action, and the expected residual risk rating following the completion of the action.

Where an entity does not propose to address a risk or recommendation, it must set out the reasons for this decision, detail any alternative actions to be taken and associated timeframes, and the expected residual risk rating following the alternative action.

Requirements for external assessors

Where a test or assessment must be undertaken by an external assessor, the requirements for the external assessor include:

- The assessor is external to the entity and, if applicable, external to the entity's corporate group.
- The assessor has not been involved in the design, implementation, operation or management of the entity's accredited services or DI data environment.
- The assessor has appropriate experience, training and qualifications to conduct the relevant assessment or systems testing. 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 (see Appendix A – Assessor qualifications in *Applying for accreditation – Guidance for organisations seeking to become accredited in Australia's Digital ID System* on the Digital ID System website).
    - Entities should consider relevant industry standards in deciding whether an assessor is appropriate for a particular assessment or test.

5.2 Annual report

Accredited entities must provide a copy of their annual report to the Regulator within 30 days of the end of their reporting period. An annual report must be accompanied by an attestation statement, signed by the entity's accountable executive, attesting that in the relevant reporting period the entity met each of its annual review and reporting requirements.

An accredited entity's annual report must include the following information and documents in line with the Accreditation Rules:

- If the entity has updated the boundaries of its DI data environment in accordance with rule 4.52, a copy of the updated documentation.
- If the entity has updated its statement of scope and applicability in accordance with rule 4.53, a copy of the updated statement.
- If the entity has conducted an assurance assessment or systems testing, a copy of the assessor's report and the entity's response.
- If the entity has conducted testing for presentation attack detection, a copy of the presentation attack detection report.
- A copy of the entity's cyber security risk assessment.
- A copy of the entity's fraud risk assessment.
- A copy of the entity's report on accessible services prepared in accordance with rule 4.48.
- A copy of the entity's report on any cyber security incidents prepared in accordance with rule 4.18.
- A copy of the entity's report on any digital ID fraud incidents prepared in accordance with rule 4.35.
- A copy of any privacy impact assessment involving the entity's accredited services or DI data environment and a copy of the entity's response to that assessment.
- For an identity service provider that conducts testing in accordance with paragraph 6.3(3)(c), of the Accreditation Rules, a copy of those test results.
- For an identity service provider that conducts testing using biometric information of an individual for testing activities, a copy of the report of that testing prepared in accordance with subrule 4.50(6).

An accredited entity is also required to include in its annual report the details of any risk treatments or recommendations that the entity has failed, or is likely to fail, to implement within the recommended timeframe (see rule 6.7).

6. Changes to accreditation

An accredited entity can apply to the Regulator to:

- vary its name
- suspend or revoke its accreditation
- vary or revoke a condition on its accreditation
- impose a new condition on its accreditation.

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

If an accredited entity is also approved to participate in the AGDIS and its accreditation is suspended or revoked, the Regulator must also suspend or revoke the entity's approval to participate in the AGDIS.

6.1 Entity initiated changes

Requesting administrative changes

An accredited entity can email the Regulator to request administrative changes.

For changes to an accredited entity's authorised officer or primary contact person/s, or an organisation's contact details, an entity should complete and submit the *Organisation and Authorised Officer form*, available on the Digital ID System website.

For changes to service contact details, an entity should complete and submit a *Service and Contact Person form*, available on the Digital ID System website.

Impose, vary or revoke conditions

An accredited entity can apply for a condition on its accreditation to be imposed, varied or revoked by using the *Conditions on Accreditation or AGDIS Approval form*, available on the Digital ID System website.

When submitting a form, an entity will need to consider:

- whether the request is for a condition to be imposed, varied, or revoked
- the desired date for the condition, or its variation or revocation, to take effect, if any
- the desired date for the condition to cease, if any
- justification for the change and relevant supporting evidence for the Regulator to consider when assessing the entity's application for the condition or the variation or revocation of a condition.

An accredited entity may wish to contact the Regulator via email to discuss the documentation required to support its application.

The Regulator may engage with the entity to discuss the purpose and proposed wording of the condition to ensure it is fit for purpose.

Once a decision has been made by the Regulator, the entity will receive a written notice of the Regulator's decision in relation to the application, stating the condition and the day on which it takes effect. If the Regulator refuses to impose, vary or revoke the condition, it must give the entity a written notice of refusal, including reasons for the refusal.

The entity must not operate in accordance with the proposed condition, its variation or revocation unless it has received the appropriate notice from the Regulator and until the effective date.

The Regulator may not provide a notice before changing a condition if the Regulator reasonably believes that the need to change the condition is serious and urgent.

The Digital ID Accredited Entities Register will be updated to reflect a decision by the Regulator to impose, vary or revoke conditions on an entity's accreditation.

Vary, suspend or revoke accreditation

An accredited entity can request to vary, suspend or revoke its accreditation.

Varying accreditation

An accredited entity can apply to change its name by completing and submitting the *Application to vary Accreditation or AGDIS Approval form*, available on the Digital ID System website.

The entity will be asked to confirm the new name they would like displayed in the Accredited Entities Register and the date they would like the change to take effect. They will also be asked to provide an attestation from an accountable executive to support the application to vary its details.

When applying to change its name, the accredited entity should provide supporting evidence of the change of the accredited entity's name, such as updated ABN Registration.

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

Suspending accreditation

An accredited entity can apply to the Regulator for a suspension of its accreditation by completing and submitting the *Suspension of Accreditation or AGDIS Approval form*, available on the Digital ID System website.

Suspension can be for a specific period, or it can be open ended.

The accredited entity will be required to provide details and reasons for requesting the suspension, dates for the requested suspension, and an attestation from an accountable executive to support the application to suspend.

The Regulator has discretion to approve or reject an entity's application for its accreditation to be suspended.

If the Regulator suspends the entity's accreditation following the entity's application, the Regulator must revoke the suspension if the entity requests the suspension be revoked.

The Regulator will issue a notice of a decision to the entity.

The Digital ID Accredited Entities Register will be updated to reflect a decision by the Regulator to suspend an entity's accreditation.

Revoking accreditation

An accredited entity can apply to the Regulator for the revocation of its accreditation by completing and submitting the *Revocation of Accreditation or AGDIS Approval form*, available on the Digital ID System website.

The accredited entity will be asked to provide details and reasons for requesting revocation and will be asked to provide an attestation from an accountable executive to support the application.

Once an accredited entity has applied for revocation of its accreditation, the Regulator must grant the request. Revocation is not instantaneous and the date the revocation takes effect will be determined by the Regulator.

The Digital ID Accredited Entities Register will be updated to reflect a decision by the Regulator to revoke an entity's accreditation.

6.2 Regulator initiated changes

Impose, vary or revoke conditions

The Regulator may on its own initiative 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 Minister for Finance may also direct the Regulator to impose new conditions on an entity's accreditation for reasons of national security.

If the Regulator intends to impose, vary or revoke a condition on its own initiative, it will provide a notice to the entity, outlining the proposed change and requesting a written response from the entity.

However, the Regulator may not provide a notice before imposing a condition if directed by the Minister for Finance or changing a condition if the Regulator reasonably believes that the need to change the condition is serious and urgent.

The Regulator may engage with the entity to discuss the purpose and proposed wording of the new or varied condition to ensure it is fit for purpose.

The Digital ID Accredited Entities Register will be updated to reflect a decision by the Regulator to impose, vary or revoke conditions on an entity's accreditation.

Suspend or revoke accreditation

The Regulator must suspend or revoke an entity's accreditation if the Minister for Finance directs it to do so for reasons of national security.

The Regulator may 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 Digital ID legislation
- the Regulator reasonably believes there has been a cyber security incident involving the entity, or a cyber security incident involving the entity is imminent (for suspension)
- the Regulator reasonably believes there has been a serious cyber security incident involving the entity (for revocation)
- the Regulator is satisfied 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

- the entity is winding up on ceasing to carry on business.

The Regulator must provide an entity with a show cause notice before suspending or revoking its accreditation. It must set out the grounds for suspending or revoking the entity's accreditation and allow the entity 28 days from the day the notice is given to respond with a written statement as to why its accreditation should not be suspended or revoked.

This provides the entity with an opportunity to engage with the Regulator and provide additional information to support its continued accreditation.

A show cause notice is not required if the reason for suspension or revocation is on the grounds of an actual or suspected cyber security incident, or if directed by the Minister for Finance.

If the Regulator decides to suspend or revoke an entity's accreditation, a written notice of suspension or revocation will be issued to the entity. The notice will include the reasons for suspension or revocation and the date it takes effect.

The Digital ID Accredited Entities Register will be updated to reflect that an entity's accreditation is suspended or revoked.

7. Compliance and enforcement approach

The Regulator exercises its compliance and enforcement powers independently and in the public interest. In deciding the appropriate compliance and enforcement response, the Regulator is guided by the ACCC Compliance and Enforcement Policy.

The Regulator may use a range of flexible and integrated strategies and tools to promote compliance with the Digital ID legislation. These include:

- engaging with accredited and approved entities to provide general information and guidance
- encouraging a compliance culture among accredited and approved entities
- working collaboratively and sharing information as appropriate with other agencies
- employing appropriate enforcement options, including by resolving possible contraventions administratively, or by litigation or other formal enforcement outcomes.

The Regulator's enforcement options are outlined in section 7.2. They include powers to impose, vary or revoke conditions on an accreditation, and powers to suspend or revoke an accreditation.

7.1 Compliance monitoring tools

The Regulator has a range of information sources and monitoring tools to assess levels of compliance with the Digital ID legislation.

These compliance monitoring tools are outlined below.

Table 1: Overview of information sources and compliance monitoring tools

	**Direct reports by consumers and stakeholders** Consumers can make reports to the Regulator through the ACCC website. Accredited and approved entities can submit reports of suspected non-compliance by other entities to the Regulator.
	**Accredited and approved entity self-reporting** Accredited and approved entities are encouraged to self-report suspected non-compliance to the Regulator.

Notification requirements

Accredited and approved entities are required to notify the Regulator of prescribed reportable incidents (see section 4.10).

Assessment of information submitted with a required notification may reveal compliance issues for further investigation or prompt re-examination of an existing accreditation or approval.

Annual review and reports

Accredited entities must conduct mandatory annual reviews and submit annual reports to the Regulator, which will assist to identify compliance issues to be addressed, as well as concerning trends (see section 5).

Cross-agency information sharing

The Regulator, System Administrator and OAIC are permitted to share information relating to potential non-compliance and have signed a tripartite MOU located on the Digital ID System website. In particular:

- The System Administrator may provide information to the Regulator regarding reportable cyber security and digital fraud incidents, IT system changes and unplanned system outages to protect the security, integrity and performance of the AGDIS.
- The OAIC may provide information to the Regulator in accordance with its functions and duties.

Undertake compliance assessments

The Regulator may issue an accredited or approved entity a notice requiring it to undergo a Compliance Assessment, in circumstances including:

- to determine if an entity is complying with the Act, or
- if the Regulator suspects a specified incident has occurred such as:
- a cyber security or digital ID fraud incident,
- an incident that may materially impact on the operation of the AGDIS, or
- a material change in the entity's operating environment that may materially impact its risk profile.

Information requests and compulsory notices

The Regulator may request that an accredited or approved entity provide information to the Regulator on a voluntary basis to assist investigations and inform compliance and enforcement activity.

The Regulator may issue compulsory notices to compel the provision of information or documents in circumstances permitted under the Act. Failure to comply with a compulsory notice may result in substantial civil pecuniary penalties under the Digital ID Act.

7.2 Enforcement action

There are a range of enforcement options available to the Regulator under the Digital ID regulatory framework. An overview of some of these options is provided in the table below.

Table 2: Overview of enforcement options

Administrative resolutions

The Regulator may decide to deal with a matter administratively. This may include:

- Drawing an issue to the entity's attention and providing information to help it gain a better understanding of the Digital ID legislation, and to encourage rectification and future compliance.
- Placing the entity on notice about the Regulator's concerns and the possibility of future investigation and action should the conduct continue or re-emerge.
- Dealing with the matter informally if the entity promptly and effectively corrects a possible contravention and implements measures to prevent recurrence.
- Accepting a voluntary written commitment to address less serious instances of non-compliance.

Infringement notices

The Regulator may issue an infringement notice where it believes on reasonable grounds that there has been a contravention of a civil penalty provision under the Act.

This may enable a matter to be resolved without legal proceedings.

Court-enforceable undertaking

The Regulator may accept a court-enforceable undertaking for a potential contravention of a civil penalty provision under the Act. The undertaking may include requirements that an accredited or approved entity will take, or refrain from taking, certain action.

This may be appropriate if the entity agrees to address the issue of concern, accepts responsibility for its actions and reviews procedures to improve compliance.

Directions

The Regulator has the power to:

- Direct an accredited or approved entity to do something or refrain from doing something, in connection with a decision related to an entity's accreditation or approval.
- Direct an approved entity to do something to protect the integrity or performance of the AGDIS.
- Direct an accredited entity to take remedial action.

Failure to comply with a direction may result in substantial civil pecuniary penalties under the Act.

Impose, vary or revoke conditions on an accreditation or approval to participate in the AGDIS

The Regulator may impose, vary or revoke conditions on the entity's accreditation or approval under certain circumstances (see section 6.2).

Suspend or revoke an accreditation or approval to participate in the AGDIS

The Regulator may suspend or revoke an entity's accreditation or approval under certain circumstances, for example if the Regulator reasonably believes the entity is breaching, or has breached, the Act (see section 6.2).

An entity is prohibited from holding out that the entity is accredited or approved in the event of a revocation.

Court action

The Regulator may commence court action where, having regard to all the circumstances, it considers litigation is the most appropriate way to achieve compliance objectives.

The Regulator may seek injunctions for breaches of civil penalty provisions under the Act and/or substantial civil pecuniary penalties.

8. Review of Regulator decisions

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

- refuse to accredit an entity
- impose, vary or revoke a condition, or refuse to impose or vary a condition on an entity's accreditation
- suspend or refuse to suspend an entity's accreditation
- revoke an entity's accreditation.

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 is eligible for internal review or 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.

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.

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.

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 entity 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 for a review of a decision is available on the Administrative Review Tribunal website.

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
- 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.

Entities may appeal to the Federal Court for judicial review of any decision of the Administrative Review Tribunal. 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.


AUSTRALIA


ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION