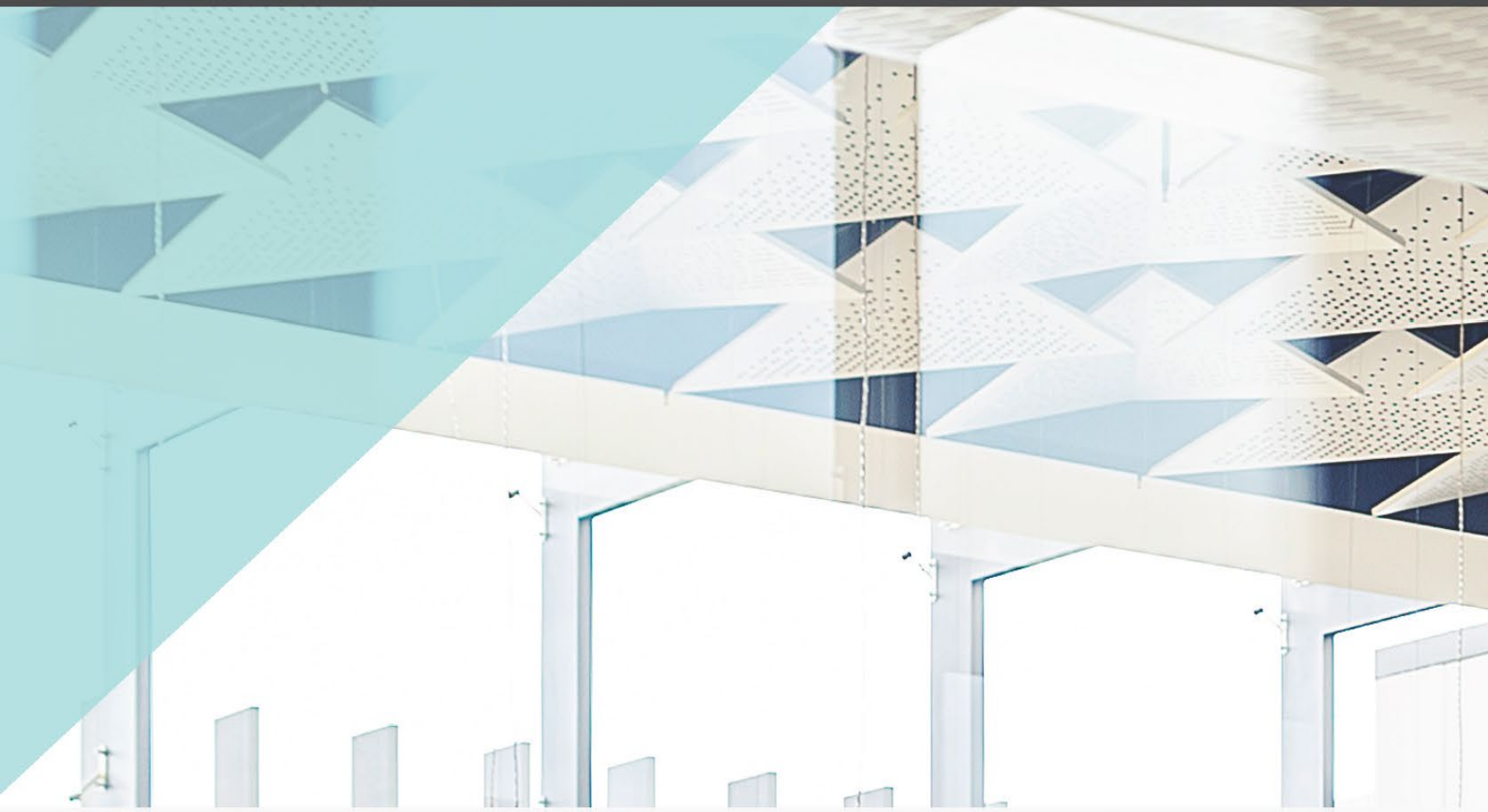
Australia's Digital ID System

Australian Government



Your Guide to the Accreditation Rules

18 September 2023

www.digitalidentity.gov.au

Department of Finance

Contents

Tables

Using this guide

This guide provides an overview of the proposed **Accreditation Rules** (the Rules) governing a voluntary **Accreditation Scheme** for providers of Digital ID services. Aspects of the Accreditation Scheme will also be controlled by the Digital ID Bill.

The Rules will be an evolution of the Australian Government's framework for its existing pilot Digital ID accreditation scheme, the Trusted Digital Identity Framework (TDIF). A range of essential privacy safeguards and security assurance benefits for Australians will be enshrined in the Digital ID Bill that applies to the Accreditation Scheme. The Accreditation Rules will be made in a legislative instrument by the Minister for Finance, under the Digital ID Bill. This will allow the Rules to be developed flexibly over time to take account of technological developments, emerging risks, and changing international standards.

This guide provides information about the Rules as compared to policy in the current published version of the TDIF to aid participants who are currently accredited under TDIF in understanding changes that may affect their operations if they choose to transition to the Accreditation Scheme. **References to the current published version of the TDIF** in this document mean version 4.8 of the TDIF, published on the Digital ID website. The Rules in this guide address feedback received from consultation with TDIF stakeholders during 2023.

This guide is not intended to be an exhaustive description of the content or changes proposed in the Rules. For a full understanding, it is recommended that you read this guide alongside the draft legislative instruments which are the authoritative description on the proposed Bill and Rules.

Full details of the exposure draft materials are contained in the draft legislative instruments available through the Consultation page.

This overview of the Accreditation Rules does not cover the Digital ID Bill or the Digital ID Rules. Please see 'Your guide to the Digital ID Bill' for further information.

Where to find more information

To help you understand more about the precursor to the Accreditation Scheme, the Trusted Digital Identity Framework, we recommend reading the resources that can be found on the Trusted Digital Identity Framework webpage.

Having your say

A set of targeted consultation questions related to specific rules are provided in each chapter of this guide. The consultation questions highlight issues raised when developing policy for the Accreditation Scheme. The consultation questions are summarised in a list in the accompanying Accreditation Rules Feedback document.

Providing feedback on the Rules

Please provide feedback on the exposure draft text of Rules as published on the Digital ID website, preferably using the Accreditation Rules Feedback document. If you wish to provide feedback on issues not covered by the consultation questions, please do so in the free text area of the Accreditation Rules Feedback document.

The consultation period for the Accreditation Rules will close 5:00 pm AEDT Tuesday 31 October 2023.

Key dates for consultation

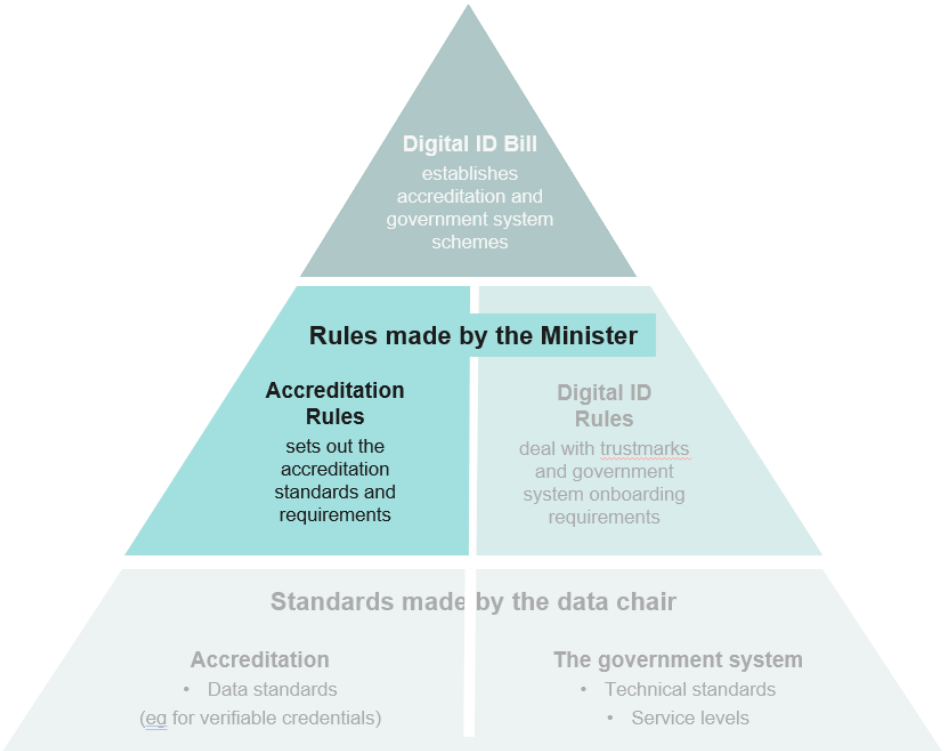
Our consultation phases for all key documents relating to the Digital ID Bill are as follows:

Document	Dates for consultation
Digital ID Bill (or Bill) and Digital ID (Digital ID) Rules (please see separate Guide)	19 September – 10 October
Accreditation Rules	19 September – 31 October

The Accreditation Rules in the context of the legislative framework

The Digital ID legislation is a package of multiple legislative instruments which govern how the Accreditation Scheme will work. The package will also govern how entities accredited in the Accreditation Scheme can participate in the Australian Government's Digital ID System if they choose to do so. The different components of the legislation are:

- **Digital ID Bill** – the primary legislation for the Accreditation Scheme, providing high-level rules for accredited Digital ID services or relying parties to participate in the Australian Government Digital ID System.
- **Accreditation Rules (the subject of this guide)** – Made by the Minister, these Rules provide the requirements for entities obtaining and maintaining accreditation in the Accreditation Scheme. These rules are a legally binding instrument which must be tabled in, and can be 'disallowed' by, Parliament.
- **Digital ID Rules** – made by the Minister, these rules provide the requirements for entities participating in the Australian Government Digital ID System. They also provide for any other general requirements, for example, Trustmark requirements and reporting. These rules are a legally binding, 'disallowable' instrument, which must be tabled in, and can be 'disallowed' by, Parliament.
- **Standards made by the Data Chair** (to be developed in future) – relate to technical integration requirements or technical features for entities in relation to accreditation, or to onboard to the AGDIS. These are legally enforceable standards published by the Data Standards Chair.



The Accreditation Rules

The **Accreditation Rules** (**Rules**) set out the rules for the Accreditation Scheme. The rules detail the controls required for an accredited entity's effective management of fraud, protective security, privacy, and usability and accessibility, as well as annual reviews to assess compliance for these controls. Additionally, the Accreditation Rules set out requirements for the operation of Digital ID services specific to the role the entity wishes to be accredited for.

The roles an entity can be accredited for are defined in Chapter 1 of the Bill. The roles are:

- **Identity Service Providers (ISP)** generate, verify, manage and maintain Digital IDs. There are two types of Digital IDs, one-off Digital IDs and reusable Digital IDs.
- **Attribute Service Providers (ASP)** verify and manage attributes. Attributes may also be bound to reusable Digital IDs.
- **Identity Exchanges (IDX)** connect other participants in a digital ID system and manage the flow of data and other information between those participants.

The Rules consist of 6 Chapters:

- **Chapter 1:** Preliminary
- **Chapter 2:** Applying for accreditation
- **Chapter 3:** Assurance assessments and systems testing
- **Chapter 4:** Maintaining accreditation
- **Chapter 5:** Role requirements for accredited entities
- **Chapter 6:** Annual reviews

Chapter 1—Preliminary

Definitions of words or terms used throughout this guide are in the Rules in **Chapter 1, rule 1.4** or at the top of the relevant chapter or rule that the definition is used in. Use of key terms and words in this guide are consistent with the Rules.

Please note the following terms in this Guide and the Rules are used to refer to entities that have applied for accreditation or are accredited:

- **Applicant** – refers to an applicant for accreditation. An entity that is not yet accredited.
- **Accredited entity** – refers to an entity that has been accredited by the Digital ID regulator (the regulator).
- **Entity** – refers to both applicants and accredited entities, where the Rules may apply to both (as is the case for Chapter 3).

Chapter 2—Applying for accreditation

Chapter 2 of the Digital ID Bill sets out the requirements to apply for accreditation.

Chapter 2 of the Accreditation Rules provides the information and documentation required to be submitted to the Digital ID Regulator (the Regulator) to be assessed for the accredited services the applicant is seeking to provide, and the matters the Regulator must consider in deciding whether to accredit an applicant.

Digital ID data environment

For the purposes of accreditation an applicant must provide a description of the entity's accredited services, how the entity will be providing those services, and a description of their **Digital ID data environment (DI data environment).** These things define the boundaries for the operational information technology system the accredited services are provided through, and the processes, policy, and personnel involved in the accredited services.

The description of the DI data environment will be accompanied by the **statement of scope and applicability** which identifies how the requirements in the Act and these rules are applied to, and assessed against, the applicant's DI data environment. The applicant will use their DI data environment description to support their claims in the statement of scope and applicability.

The DI data environment and the statement of scope and applicability are living documents, which are required to be reviewed and updated during the annual review process in **Chapter 6** of the Rules.

Privacy Impact Assessment (PIA)

Applicants are required to submit a PIA which has been conducted according to **rule 2.3.** A PIA assesses the privacy impact and risks to the applicant's DI data environment and accredited services. Additionally, it assesses the entity's compliance with **Privacy Safeguards in Chapter 3 of the Bill** and the **privacy rules in Chapter 4, Part 3 of the Rules**.

For more information about the requirements for entities to submit PIAs please see **rule 2.3** of the Accreditation Rules. For more information about when PIAs are required to be conducted by the Privacy Code, see the *OAIC Guide to undertaking privacy impact assessments*.

Further information links:

- OAIC Guide to undertaking privacy impact assessments.

Chapter 3—Assurance assessments and systems testing

Chapter 3 Assurance assessments and systems testing of the Rules sets out the requirements to conduct assurance assessments and systems testing to review and assess if the elements of the DI data environment meet the requirements of the Act and these rules. Applicants and accredited entities are required to conduct assurance assessments and systems testing as part of their application for accreditation (set out in **Chapter 2 of the Rules**) and as part of their ongoing annual review obligations (set out in **Chapter 6 of the Rules**).

Change from current policy:

- (New) introduction of a fraud assessment to assess an entity's compliance with the fraud control rules in **Chapter 4, Part 2** of the Rules.
- (New) introduction of a usability and accessibility assessment to assess an entity's compliance with the usability and accessibility rules **Chapter 4, Part 4**.
- (Changed) Web Content Accessibility Guidelines (WCAG) testing is no longer required to be completed yearly and by an independent assessor.
- (Changed) Removal of a separate privacy assessment. The new rules for entities to comply with the Privacy Code and the requirements for an applicant to conduct a PIA require that the PIA includes an assessment of the entity's compliance with relevant privacy requirements in the Bill and the Rules.

Assessor requirements

Assurance assessments and systems testing must be conducted by an assessor that meets the requirements set out in **Chapter 3, Part 1** of the Rules.

Rule 3.1 sets out the scope of the assurance assessment or systems testing for the entity's DI data environment that are being assessed or tested. **Rule 3.2** sets out the requirements for the assessor that will conduct the assurance assessment or systems testing. Additional requirements for the assessor of a particular type of assessment or systems testing are contained in the specific rules for that assurance assessment or systems testing. For example, **rule 3.7(2)** requires that the assessor for a fraud assessment be external to the entity or its corporate group and independent from the design, implementation, operation and management of the entity's DI data environment.

Assurance assessment and systems testing rules

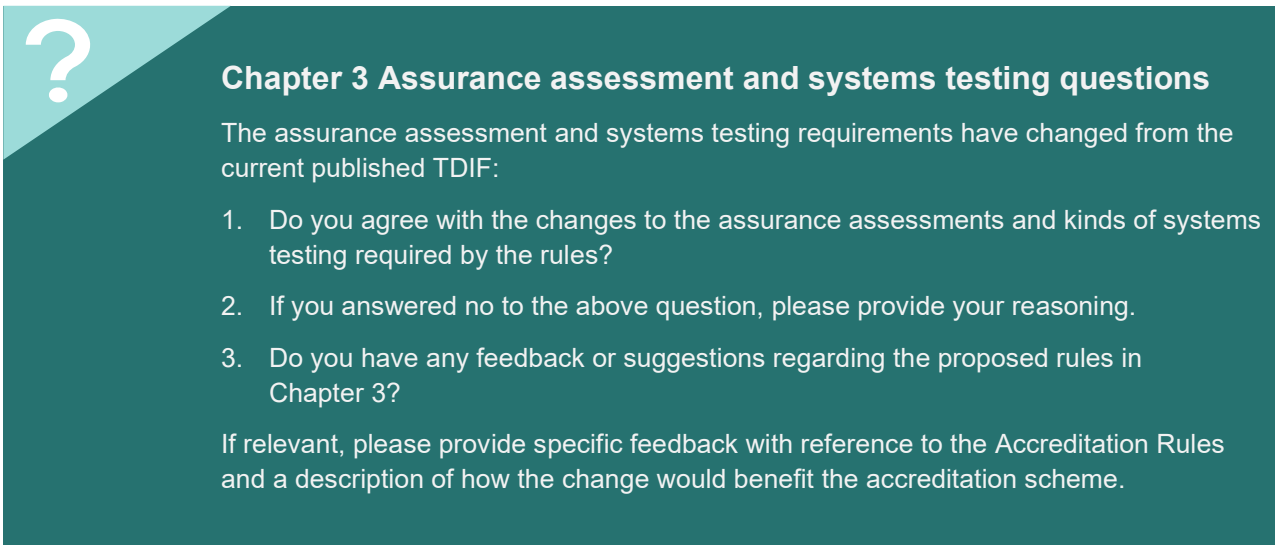
An applicant must undertake all assurance assessments and systems testing set out in **Chapter 3 of the Rules**, except for **rule 3.12** which sets out the requirements for usability testing. Only entities with public-facing accredited services must conduct usability testing. For example, an identity exchange provider may provide its services to other participants of a digital ID system in such a way that individuals will never know it is there because it does not provide a public-facing accredited service. Such a service is not required to conduct usability testing.

An accredited entity must undertake assurance assessments and systems testing in **Chapter 6 of the Rules**.

Table 1 – assurance assessment and systems testing summary sets out a summary of the assurance assessment and systems testing schedule for entities, including the additional assessor rules. This table is provided for guidance purposes only.

Table 1 – Assurance assessment and systems testing summary

Assessment or systems testing	Additional assessor requirements	Required for applicants? (see chapter 2 of the rules)	Frequency for accredited entities (see Chapter 6 of the rules)
Privacy Impact Assessment (PIA). See rule 2.6	See rule **2.3 (2)(b)**	Yes	See: OAIC advice when do agencies need to conduct a privacy impact assessment.
Protective security assessment. See rule 3.4	See **rule 3.4 (2)**	Yes	Every 2 years. See **rule 6.3 (3)** OR As per material changes to the DI data environment. See **rule 6.2**
Fraud assessment. See rule 3.7	See **rule 3.7 (2)**	Yes	Every 2* years. See **rule 6.3 (1)** *see **rule 6.3 (2)** for exceptions to the additional assessor requirements in **rule 3.7 (2)** OR As per material changes to the DI data environment. See **rule 6.2**
Usability and accessibility assessment See rule 3.8	-	Yes	As per material changes to the DI data environment. See **rule 6.2**
Penetration testing See rules 3.9, 3.10 and 3.11	See **rule 3.10 (1)**	Yes	Every year. See **rule 6.4 (2)**
Usability testing See rules 3.12 and 3.13	-	Yes, where the entity public-facing accredited services.	As per material changes to the DI data environment. See **rule 6.2**
WCAG testing See rules 3.14 and 3.15	-	Yes	As per material changes to the DI data environment. See **rule 6.2**



Chapter 3 Assurance assessment and systems testing questions

The assurance assessment and systems testing requirements have changed from the current published TDIF:

1. Do you agree with the changes to the assurance assessments and kinds of systems testing required by the rules?
2. If you answered no to the above question, please provide your reasoning.
3. Do you have any feedback or suggestions regarding the proposed rules in Chapter 3?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

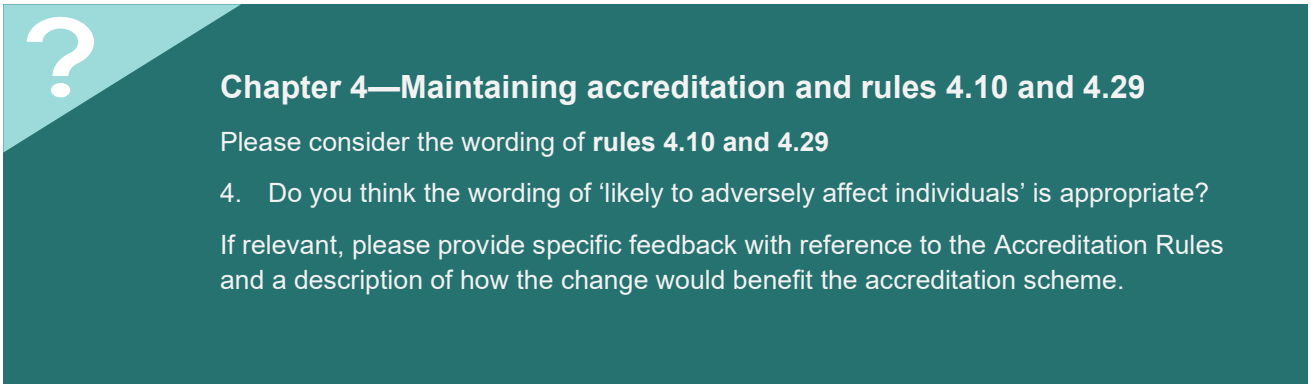
Chapter 4—Maintaining accreditation

Chapter 4 of the Rules includes ongoing requirements all accredited entities must meet to maintain accreditation. This includes requirements across the domains of privacy, fraud control, protective security, usability and accessibility and reportable incidents.

Accredited entities have an obligation to manage risks by maintaining and improving their governance and technical capabilities relevant to each of the above domain, for their accredited services and DI data environment.

Advice to Individuals

Rules 4.8 and **4.27** require that accredited entities notify individuals where a cyber security or Digital ID fraud risk or incident is *likely* to adversely affect individuals using their accredited services. This means that accredited entities are required to warn individuals of scams or other malicious attacks aimed at compromising their Digital ID or attributes as related to the accredited services of the entity where those scams or malicious attacks will result in adverse affects.



Protective security

Chapter 4, Part 1 of the Rules contains the protective security requirements for accredited entities. Accredited entities are required to have and maintain a protective security capability that demonstrates they can manage the protective security of their DI data environment. This includes ensuring that its DI data environment is appropriate and adapted to respond to cyber security risks and emerging risks that impact its DI data environment.

Protective security frameworks

Change from current policy: the current published TDIF protective security requirements were based on several different sources, including:

- The Australian Government's Protective Security Policy Framework (PSPF)
- The Australian Cyber Security Centre's Information Security Manual (ISM)
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements and ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.
  - For the purposes of this Guide, these two ISO/IEC standards will be referred to collectively as ISO 27001.

Rather than continue to duplicate requirements in these frameworks, which is labour and skills intensive, all protective security requirements that have equivalent ISO 27001 and PSPF controls have been removed. Accredited entities must comply with and are assessed against these frameworks instead.

- For entities that implement the PSPF: the required controls are listed at Schedule 2 in the Rules.
  - please note that some requirements and sub-requirements have been purposefully omitted as they are only applicable to Australian Government entities bound by the PSPF.
- For entities that implement ISO 27001, the entity must comply with all controls in ISO 27001 and controls listed in Appendix A of that document, which correspond to all controls in ISO 27002.

Entities may also choose to be assessed against an equivalent protective security framework, as long as that framework contains equivalent protective security controls to either the PSPF or ISO 27001.

An entity that chooses to apply controls against an alternative framework must map those controls against either PSPF or ISO 27001 and submit this evidence to the Regulator.

Chapter 4, Part 1, Division 2 sets out the rules for protective security frameworks.

Further information links:

- Protective Security Policy Framework (PSPF)
- Australian Cyber Security Centre's Information Security Manual (ISM)
- the ISO 27001 series.

ISO 27001: 2013 to 2022 transition timeframe

The latest version of the ISO 27001 controls was released in 2022. This was a major update and as such, ISO certification bodies have advised that entities certified under the framework be given until November 2025 to transition to the updated controls. However, the current advice to entities is that they are encouraged to transition their certification sooner rather than later.

Due to the sensitive nature of Digital ID information and potential protective security risks involved, **rule 4.3 (2)** requires that current accredited entities and any new accredited entities that are certified under ISO 27001: 2013 must transition their certification and compliance with ISO 27001: 2022 **by 31 December 2024**.

Chapter 4—Maintaining accreditation rule 4.4 (2)

5. Do you agree with this transition timeframe?
6. Are there any risks or issues with this transition timeframe?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Additional protective security controls

Additional protective security rules in **Chapter 4, Part 1, Division 3** are either bespoke controls particular to the protective security of Digital IDs or are rules that occur in one framework but not the other. Where

the rule is a duplicate of a framework control, it does not need to be assessed again during the protective security assessment.

Essential Eight

Change from current policy: in the current published TDIF, entities are required to implement four out of the Essential Eight strategies to mitigate cyber security incidents. This requirement is based on an old version of the PSPF. PSPF Policy 10 was updated in 2022 to mandate that entities must implement the Essential Eight.

Rule 4.17 sets out the obligation for accredited entities to comply with the Strategies to Mitigate Cyber Security Incidents document for strategies marked 'essential' in the relative security effectiveness rating column of the table. This rule provides the high-level requirements an accredited entity must implement, and that the independent assessor will review as part of the protective security assessment.

Rule 3.5 describes the essential strategies review reports that must be conducted by entities. This report is a self-assessment of the entity's compliance with controls in the ISM that map to the Essential Eight. This self-assessment report aims to complement **rule 4.17** and assist the independent assessor to assess an entity's compliance with the high-level Essential Eight requirements.

Further information links:

- Essential strategies to mitigate cyber security incidents
- Essential Eight Maturity Model to ISM mapping
- Essential Eight Assessment Process Guide

Chapter 4—Maintaining accreditation: Essential Eight rules 4.18 and 3.4

7. Do you agree with the implementation of the new Essential Eight requirements as currently drafted in the Accreditation Rules?
8. If you answered no to the above question, please provide your reasoning.
9. Do you have any feedback or suggestions regarding the Essential Eight rules?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Cloud service management (new rule)

Cloud services have become an important and prevalent technology used in Digital ID services and as such require appropriate security management. **Rule 4.12** outlines obligations for accredited entities regarding the selection, use and management of cloud service providers. This rule is based controls for cloud service management as set out in the *Guidelines for Procurement and Outsourcing* chapter of the *ISM* and ISO 27001: 2022 Table A.1 control 5.23.

Note: this new rule corresponds to ISO 27001 2022 Table A.1 control 5.23 for effective and secure cloud service management. Entities that implement ISO 27001 2022 are not required to have this control assessed in addition to the ISO 27001 2022 Table A.1 control 5.23.

Further information links:

- Guidelines for Procurement and Outsourcing chapter of the ISM

Other updates and changes

Several protective security rules have been consolidated and clarified, including:

- **Rule 4.18—**Logging requirements for accredited entities.
- **Rule 4.15—**Disaster recovery and business continuity management, including obligations related to the management of recovery and restoration of backups.
- **Rules 4.19** and **4.20—**Approved cryptography. This includes a new carve out for the use of approved cryptography regarding the use of Transport Layer Security (TLS) in the required Australian Signals Directorate Approved Cryptographic Algorithms (AACA) and Australian Signals Directorate Approved Cryptographic Protocols (AACP). Requirements for the operation of approved cryptography corresponds to controls in the ISM regarding AACAs and AACPs.
- **Rule 4.21—**Cryptographic key management processes and procedures.

Chapter 4—Maintaining accreditation : protective security rules

10. Do you have any feedback regarding the proposed updates to the protective security rules?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Fraud

Chapter 4, Part 2 of the Rules outlines the fraud control requirements for accredited entities. Accredited entities are required to have and maintain a fraud capability that complies with the fraud rules and is appropriate and adapted to respond to the fraud risks that exist or may exist in the entity's operational environment.

Accredited entities are required to identify, treat and manage fraud risks to their accredited services. Additionally, entities must take reasonable steps to prevent, detect and deal with digital identity fraud incidents.

Change from current policy: The fraud rules have been streamlined and updated for consistency with the protective security rules. Rules regarding the suspension and deactivation of Digital IDs or attributes where a fraud incident occurs are now located:

- For Identity Service Providers (ISP), **Chapter 5, Part 2, Division 2, rules 5.7 to 5.9**.
- For Attribute Service Providers (ASP), **Chapter 5, Part 3, Division 2, rules 5.39 and 5.40**.

The current published TDIF requirement *FRAUD-02-04-02b* has been redrafted into the sections of the rules for ISPs and ASPs as outlined above.

TDIF Req: FRAUD-02-04-02b; Updated: Mar-22; Applicability: A, C, I

If the Applicant reasonably suspects that a Digital Identity is fraudulent or its use may result in a Digital Identity Fraud Incident, the Applicant:

a) MUST NOT allow a new registration or update of that Digital Identity to be completed; and

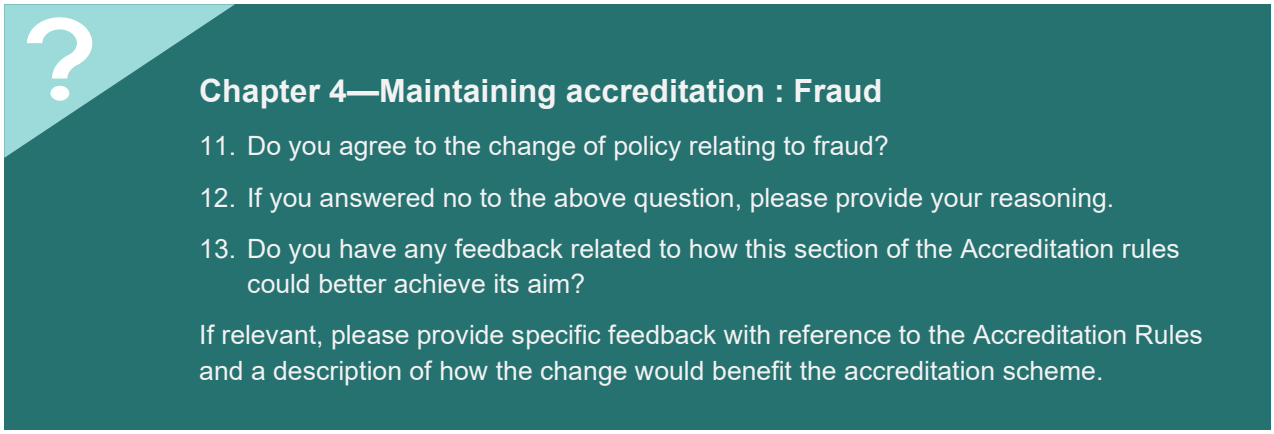
b) MUST block the use of the Digital Identity on its Identity System.

Consultation note: The previous TDIF requirement was unclear in its meaning of 'reasonably suspects'.

Additionally, the immediate actions of not allowing a new registration or update and then blocking the Digital ID from the ISP or ASP's DI data environment or the use of it across a digital ID system are unsatisfactory. These requirements do not consider the individual who may be caught up in a false positive suspected Digital ID fraud incident.

The Rules provide a clearer and more considered process.

Where an entity flags the Digital ID as being involved in a *suspected* fraud incident, there is now an obligation for the accredited entity to take reasonable steps to check that the Digital ID continues to be under the control of the individual to whom the Digital ID relates. This means before a Digital ID is suspended and the individual is required to conduct the entire identity proofing process again or embark on the recovery process, the accredited entity may be able to confirm that the Digital ID is not involved in a suspected or actual fraud incident.



Privacy

Australian Privacy Principles (APPs)

Accredited entities must comply with the Australian Privacy Principles (or APPs). The APPs are the cornerstone of the privacy protection framework in the *Privacy Act 1988*.

Broadly, the principles govern standards, rights and obligations related to:

- open and transparent management of personal information
- the collection, use and disclosure of personal information (including sensitive information)
- an organisation or agency's privacy governance and accountability
- integrity and correction of personal information (including reasonable steps to protect the security and quality of personal information)
- and the rights of individuals to access their personal information.

Further information links:

- Office of the Australian Information Commissioners OAIC

Privacy Governance Code

Rule 4.35 sets out the requirements for accredited entities to comply with the Privacy Governance Code (Privacy Code) for Australian Government Agencies.

Change from current policy: The current published version of the TDIF includes requirements from the Privacy Code but does not require that entities comply with it.

Primarily, the Privacy Code requirements include that an accredited entity must:

- have a Privacy Management Plan
- have a Privacy Officer to fulfill functions that manage and mitigate potential privacy risks in the DI data environment
- have a Privacy Champion
- conduct PIAs in accordance with the Privacy Code
- have and maintain an internal privacy capability including:
  - privacy education and training for personnel whose duties relate to the accredited service, including third parties; and
  - regular reviews of internal privacy processes specific to the DI data environment.

Further information links:

- Privacy Code: Australian Government Agencies Privacy Code | OAIC

Privacy Act review

The *Privacy Act 1988* was recently reviewed by the Attorney-General's Department with the final report released on 16 February 2023.[1]

Consideration of the recommendations of the review is underway and may lead to amendment of the *Privacy Act 1988* which may impact responsibilities under the *Privacy Act 1988* including the formulation and application of the APPs and the Privacy Governance Code.

Data minimisation principle

The data minimisation principle **rule 4.38** requires accredited entities minimise collection and disclosure of personal information in connection with its accredited services.

This means an accredited entity must only disclose personal information to a relying party or participating relying party if it is satisfied disclosure of that personal information to the party is reasonably necessary for the party to provide its service or access to its service to the individual.

[1] Privacy Act Review Report | Attorney-General's Department (ag.gov.au), https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

Accredited entities must take reasonable steps to ensure that requests for personal or sensitive information are reasonably necessary to reduce not only the collection of personal information but the risks of a data breach of that information.

An example of data minimisation may be where a relying party needs to confirm that an individual purchasing alcohol online is over the age of 18. The relying party may not need to know the name of the individual, the birth date of that individual or any details other than whether the individual is over the age of 18. This may be satisfied by an accredited service with a confirmation that the Digital ID has been verified to an appropriate IP level and that the individual is confirmed to be over 18 – a yes/no answer.

Change from current policy: The data minimisation principle aims to enhance the privacy protections for individuals using their Digital ID and minimise the proliferation of data across the digital economy by ensuring that relying parties reasonably need such information to provide the service, and where possible minimising what is sent through a digital ID system. This also aims to remove the current prohibition on ISPs from collecting and disclosing attributes outside a limited subset of attributes and restricted attributes referred to in tables 2 and 3 and *Section 3.6 Attribute collection, verification and validation* of the TDIF 05 Role Requirements.

Chapter 4—Maintaining accreditation : rule 4.38

Please refer to the draft wording of the data minimisation principle in **rule 4.38** of the Rules.

14. Do you agree that the data minimisation principle as drafted is able to satisfy the aims outlined above?
15. If you answered no to the above question, please provide your reasoning.
16. Are there any specific risks or issues with the rule as drafted?
17. What are your recommendations (if any) to improve the data minimisation principle?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Retention and use of biometric information

Chapter 4, Part 4, Division 2 outlines the rules that apply to accredited entities that are authorised to collect biometric information under section 45 of the Digital ID Bill, where the accredited entity retains that biometric information for fraud or testing purposes up to 14 days after it is collected.

Rules 4.43 and 4.44 require entities holding biometric information to follow a set of ethical principles aiming to avoid disadvantage to, or discrimination against, individuals.

Chapter 4—Maintaining accreditation : rules 4.43 and 4.44

Please consider **rules 4.43 and 4.44.**

18. Are there any international standards for ethical policies or plans that you think entities must take into account when retaining and analysing biometric information for the purposes of fraud detection, prevention or investigation?
19. Do you have any suggestions or feedback regarding the Rules for the safe retention of biometric information for fraud or testing purposes?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Usability and accessibility

User experience and accessibility is a key consideration of the accreditation process. **Chapter 4, Part 5** describes the usability and accessibility rules. The Rules have been clarified and consolidated by ensuring that they are scoped appropriately to apply to an entity's public-facing accredited services (for example, where the accredited service is delivered to individuals via a public-facing app) or public-facing information related to their accredited services (such as a privacy policy on an accredited entity's website). Where possible, duplicate or confusing requirements have been removed to ensure a streamlined approach to usability and accessibility.

Web Content Accessibility Guidelines (WCAG)

Change from current policy: an accredited entity's obligations to comply with WCAG has been updated to include feedback from the pilot accreditation program and consider updates to the WCAG framework and controls. The current published TDIF differentiates between WCAG 2.0 and 2.1 depending on the kind of service delivery method for the accredited entity's services (i.e., web or app).

Rule 4.46 states that accredited entities must take reasonable steps to ensure that all user-facing information that relates to an entity's accredited services is compliant with WCAG 2.1 to the AA standard. This means that where an individual is interacting with information about or regarding the entity's accredited services (such as on the accredited entity's website for a privacy policy, or in an accredited ISP's Digital ID app), the entity must take reasonable steps to ensure the information is displayed and compliant with WCAG 2.1 to the AA standard.

Chapter 4—Maintaining accreditation : Web Content Accessibility Guidelines (WCAG) rule

20. Do you agree with the updated WCAG rule?
21. If you answered no to the above question, please provide your reasoning.
22. Do you have any feedback or suggestions regarding the updated WCAG rule?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Chapter 5—Role requirements for accredited entities

Accredited Identity Service Providers (ISP)

Children and Digital IDs

The Bill aims to strike a balance between protecting children who may be unable to provide informed consent when creating and using a Digital ID and empowering them to access the services they need independently.

The Bill will give the Minister flexibility to make rules specifying an age for children to create a Digital ID. The rule making power will allow for flexibility to respond to changes across other regimes dealing with age. The Rules prohibit an identity service provider from creating a Digital ID for an individual under 15 years. However, it is proposed the Rules be changed to prohibit an identity service provider from creating a Digital ID for an individual under 14 years. This would maintain consistency with other schemes. The proposal is subject to consultation feedback and *Age Discrimination Act 2004* compliance.

Rule 5.2 requires that Accredited ISPs must not generate a Digital ID for an individual under the age of 15. it is proposed Rule 5.2 be changed to prohibit an identity service provider from creating a Digital ID for an individual under 14 years.

?

Chapter 5—Role requirements for accredited entities : Digital IDs for children

23. Do you agree with the inclusion of this rule for accredited identity service providers?
24. Do you agree with the age of consent for the creation and use of a Digital ID being changed to 14 years of age?
25. If you answered no to the above questions, please provide your reasoning.

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

One-off Digital IDs

A one-off Digital ID is generated and verified for one-time use. Once the individual has verified their identity and any information is disclosed to the relying party, any personal information related to the transaction other than as required by the Rules (such as transaction logging information) must be destroyed by the accredited entity.

Change from current policy: the current published TDIF does not contain specific requirements for the accreditation of one-off Digital IDs. Feedback from the pilot accreditation program has informed the new rules for one-off Digital IDs.

Chapter 5, Part 2, Division 1 of the Rules describes the requirements for one-off Digital IDs.

Chapter 5—Role requirements for accredited entities : one-off Digital IDs

26. Do you agree with the inclusion of one-off Digital IDs?
27. If you answered no to the above question, please provide your reasoning.
28. Are there any risks or issues with the controls for the one-off Digital ID service?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Reusable Digital IDs

The rules for the effective management and operation of a reusable Digital ID have been clarified and consolidated into a separate division for readability. This includes moving certain fraud management rules around the suspension and reactivation of Digital IDs from the Fraud section to the reusable Digital ID section as they were only applicable to ISPs (please see the Fraud section above for further explanation).

Change from current policy: *Section 3.6 Attribute collection, verification and validation* in the current published TDIF has been removed from the Rules (page 18, TDIF 05 Role Requirements). This includes Tables 2 and 3, which described which attributes an ISP was restricted to collect, verify and disclose. This restriction has been replaced by the data minimisation principle, located in **rule 4.38** of the Rules. Please see the privacy section of this guide above for further explanation regarding the data minimisation principle.

Identity proofing standards for Digital IDs

The identity proofing rules have been clarified and consolidated into a separate division for readability. The identity proofing standards sets out the entire identity proofing process that all ISPs must comply with when conducting identity proofing. It consists of **Chapter 5, Part 2**:

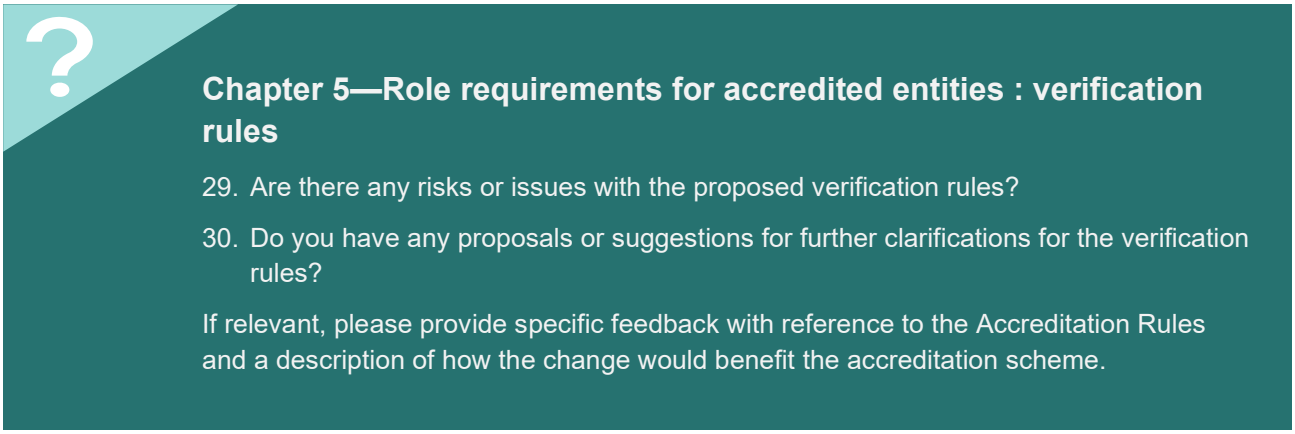
- **Division 3** sets out the general identity proofing requirements including **Table 1** Identity proofing levels and requirements for each level. The types of accepted identity credentials referenced in Table 1 can be found in **Schedule 1** Credential Requirements.
- **Division 3, Subdivision 1—Verification rules** sets out the requirements for the accepted verification methods for credentials, attributes and restricted attributes. These rules are used for both ISPs and ASPs.
- **Division 3, Subdivision 2—Biometric binding** sets out the requirements for how accredited entities must carry out biometric binding, which is required to meet IP levels 2 Plus, 3 and 4. The biometric binding process includes four different methods of accepted biometric matching: Source biometric matching, Technical biometric matching, eIDVT and Manual Face Comparison.
- **Division 3, Subdivision 3—Biometric testing** sets out the testing standards for the biometric matching processes. Where applicable, ISPs must have their chosen biometric binding process tested. Various components of the method may require separate testing.
- **Division 3, Subdivision 4—User experience** sets out the user experience rules for ISPs.
- **Division 3, Subdivision 5—Requirements for alternative proofing processes** sets out the requirements for ISPs to comply with if they wish to implement an alternative proofing process. The alternative proofing process must be approved by the Digital ID Regulator and will be a condition on the ISP's accreditation.

Verification rules

Change from current policy: Identity proofing requires ISPs to verify the attributes on credentials listed in the **Schedule 1** of the Rules. Additionally, ASPs are required to verify attributes as part of their accredited service. The current published TDIF does not contain requirements for how verification of these credentials or attributes are carried out, apart from what is contained in the definitions of the verification methods.

There are three types of verification methods: source verification, technical verification and visual verification.

New rules in **Chapter 5, Part 2, Division 3, Subdivision 1** have been included to clarify how verification of credentials and attributes must be carried out by an ISP or ASP. Technical verification has been clarified to include explicit reference to controls related to public key infrastructure (PKI) technology required for it to be carried out on credentials and attributes.



Please note that these rules will be considered in line with proposed updates to the National Identity Proofing Guidelines and any future verifiable credential policy.

Other changes

Change from current policy: The approved authentication bindings for each IP level have been updated (**Table 1, item 14**). This is a single change to ensure that where a reusable Digital ID is IP1 Plus, the approved authentication binding level is Authentication Level 2 (AL2). This is because an IP1 Plus Digital ID may contain verified personal or sensitive information. The PSPF Policy 10 and Essential Eight controls advise that personal and sensitive information that can be accessed via the internet is protected by multi-factor authentication. Additionally, NIST 800-63b requirements—on which the authentication management standard rules are modelled off—mandate AL2 is used where personal information is made available online.

electronic Identity Verification Technology (eIDVT)

Change from current policy: In the current published TDIF, higher IP levels require confirming the link between an individual and a claimed identity using biometrics – referred to as biometric binding. Currently, biometric binding can only be achieved through a relatively restricted set of pathways that require a user to have a valid Australian ePassport or to perform an in-person transaction (e.g., visiting a service centre in-person). This is partly due to the methods and types of credentials that are issued in Australia, as well as the availability of services to verify biometric images contained on or within credentials.

Rule 5.24 is a new rule for the inclusion of eIDVT (electronic Identity Verification Technology) biometric matching as one of the approved biometric binding methods for **identity proofing level 2 Plus ONLY.**

This involves defining a new pathway for achieving biometric binding and facilitating greater inclusion and uptake of Digital IDs in Australia.

This type of biometric matching was consulted on for inclusion in the TDIF in late 2021 and at the time there was no available testing standard or metrics for eIDVT solutions. As such, it was not included in the TDIF at the time, despite the technology's widespread use in the private sector.

Since then, FIDO (Fast Identity Online) has released a new standard for the testing of eIDVT solutions. FIDO is an internationally recognised open industry association that issues standards related to verification and authentication. In the Rules, *FIDO Document Authenticity Requirements* refers to the requirements for testing eIDVT solutions as developed by FIDO and published in August 2022. This standard provides the testing methods and metrics that eIDVT solutions must meet. **Rule 5.32** describes the testing metrics and standard an ISP must meet to provide eIDVT biometric matching at IP2 Plus.

Further information links:

- FIDO Document Authenticity Verification Requirements

Document liveness testing rules for eIDVT

The current published version of the *FIDO Document Authenticity Requirements* does not contain rules for the testing of document liveness. As part of including eIDVT in the identity proofing standard, biometric and security experts were engaged to develop rules and a test standard for the operation of document liveness as part of eIDVT biometric matching. Please note that when FIDO updates the standard, these proposed rules will be reviewed for duplication.

Rule 5.31 describes the testing requirements for document liveness.

What is document liveness?

eIDVT systems may include multiple technology elements including optical character recognition (OCR) and computer vision algorithms. The problem of detecting fraudulent or altered identity documents using exclusively non-original samples – referring to photographs or scans of original documents – can be exceptionally challenging, with large variability between well-performing and poorly performing solutions available in the marketplace.

By ensuring eIDVT systems perform a 'liveness check' (i.e., a check for the presence of the document) of the identity document presented to a device's camera, this process ensures that the original physical document is present at the point of identity verification. This is similar to the way liveness detection for individuals is performed using presentation attack detection technology. An additional liveness check is a particularly appealing control in 2023, where databases containing personal information and document information (such as passport numbers) have been breached and leaked online. By verifying the presence of the physical document at the point of identity verification, attacks based solely on breached database information may be mitigated. Any potential attacks would be required to also produce convincing fraudulent document samples based on the fraudulently obtained genuine document information. This is a prohibitive, difficult, and time-consuming task which may deter many types of attackers.

Chapter 5—Role requirements for accredited entities : eIDVT and liveness rules

31. Do you agree with the inclusion of eIDVT as a biometric matching method at IP2 plus only?
32. If you answered no to the above question, please provide your reasoning
33. Are there any risks or issues with the proposed inclusion of eIDVT as a biometric matching method at IP2 Plus only?
34. What are your thoughts on allowing eIDVT to meet the biometric binding requirements for IP3?

Chapter 5—Role requirements for accredited entities : eIDVT and liveness rules (continued)

35. Are there any risks or issues with the proposed rules regarding the testing of eIDVT? Please refer to specific rules in your feedback where possible.
36. eIDVT has been restricted to Australian drivers licences and Australian passports. Do you think it should be expanded to other credentials in **Schedule 1 Credential Requirements** (such as proof of age cards)?
37. eIDVT could be used for the verification of foreign identity credentials in the future, do you think there is room to expand the Digital ID identity proofing rules to include the proofing of foreign credentials?
38. Do you have any feedback or suggestions regarding the proposed document liveness rules?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Biometric testing standard

Change from current policy: the current published TDIF has the biometric testing requirements contained in each section for the type of biometric matching method. With the introduction of eIDVT, this means that some testing rules are shared by different biometric matching methods. These testing rules have been consolidated in a separate division for ease of reference.

Table 2: testing required for biometric binding provides an overview of what kind of testing is required for each type of biometric matching method. This is provided as guidance only.

Table 2 testing requirements for biometric binding

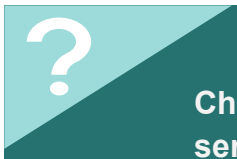
Rules	Technical Biometric Matching	Source Biometric Matching	eIDVT	Manual Face Comparison
5.28 Testing of presentation attack detection technology	Yes, if using online biometric binding	Yes, if using online biometric binding	Yes, if using online biometric binding	-
5.29 Testing of biometric matching algorithm	Yes	-	Yes	-
5.30 Source biometric matching testing	-	Yes	-	-
5.31 Testing for document liveness	-	-	Yes	-
5.32 Testing requirements for eIDVT	-	-	Yes	-

Attribute service provider (ASP) rules

Change from current policy: the rules for ASPs have been consolidated and updated in accordance with feedback from the pilot accreditation program. The aim of the updates to the ASP rules is to provide greater flexibility in how ASPs are accredited. In particular, the attribute classes have been removed from the Rules and replaced with rules requiring that an ASP provides verified attributes. Further clarifications have been added regarding an ASP's representation of the data provenance of verified attributes.

See **Chapter 5, Part 3** for the Rules relating to ASPs.

Additionally, the Rules for binding attributes to reusable Digital IDs and the intersection these rules have with the Authentication Management Standard have been clarified (see **Chapter 5, Part 3, Division 2**). These rules are only applicable where an individual wishes to bind a verified attribute to their Digital ID and the ASP has the technical capability to do so.



Chapter 5—Role requirements for accredited entities : attribute service provider rules

39. Do you have any feedback or suggestions regarding the proposed rules for ASPs?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Authentication management standard

Chapter 5, Part 4 of the Rules contains requirements for authentication management. These rules are shared by both ISPs and ASPs where related to reusable Digital IDs, or attributes bound to reusable Digital IDs respectively. There are requirements for how certain technology required for the provision of accredited services must work. These requirements will likely be lifted out of the Rules and into a data standard to ensure that they are consistently updated in accordance with best-practice international standards or technology advancement.

Change from current policy: The current published version of the TDIF contains rules for an additional role known as a Credential Service Provider (CSP). The terminology of the TDIF also refers to authenticators as credentials, which is not aligned with common usage and international standards. Following a targeted consultation with key stakeholders and feedback from the pilot accreditation program, the role of a credential service provider has been removed from the Bill and the Accreditation Rules. It has been replaced by **Chapter 5, Part 4.**

Definitions and language regarding credentials have been changed. Please refer to the definitions and interpretation sections of the Rules in **rule 1.4**.

Biometric authentication updates (in-device authentication)

Feedback from the pilot accreditation program and wider Digital ID landscape has indicated the wide use of in-device biometric capability provided by smartphone Original Equipment Manufacturers (OEM) (e.g., Apple, Samsung, etc). The current published TDIF is silent on this type of biometric for authentication method and presupposes the use of a bespoke solution (see **rule 5.58**) operated by the ISP.

Chapter 5, Part 4, Division 4 of the Rules have been updated to incorporate in-device biometric capability for biometric authentication.

Changes from current policy:

- Defining and explicitly allowing the use of in-device biometric capability for biometric authentication.
- Providing rules for the use of in-device biometric capability:
  - can only be used as a factor in a multi-factor authenticator (as defined by the Rules)
  - cannot be used at Authentication Level 3 (AL3)
  - does not require independent testing by a biometric testing entity
- Updating the PAD and biometric matching algorithm testing requirements to align with current best practice and the Biometric Binding requirements.

The major change introduced is to explicitly allow the use of in-device capability at AL1 and AL2 as a biometric factor for multi-factor authenticators.

Biometric authentication in-device capability is restricted to AL1 and AL2, and does not require any independent testing. This is due to the trust placed in the OEM in-device capability to operate to high standards and having been tested prior to release.

Table 3: testing requirements for biometric authentication

Authentication Level	In-device biometrics allowed?	Testing of in-device biometrics	Custom biometrics allowed?	PAD and biometric matching algorithm testing of custom biometrics
AL1	Yes	Not required	Yes	In-house or independent testing entity
AL2	Yes	Not required	Yes	Independent testing entity only
AL3	No	N/A	Yes	Independent testing entity only

Chapter 5—Role requirements for accredited entities : in-device biometric capabilities

40. Do you agree with the inclusion of in-device biometric capability as a method of unlocking authentication factors up to AL2?
41. If you answered no to the above question, please provide your reasoning.
42. Do you have any feedback or suggestions regarding the proposed rules for the inclusion of in-device biometric capability for authentication?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Identity exchange rules

Chapter 5, Part 5 of the Rules has been updated to clarify the identity exchange's responsibilities and assurances regarding its role in conveying, managing or coordinating information between participants of a digital ID system.

The new rules draw on findings from the pilot accreditation program and aim to strengthen the assurances around the accreditation of identity exchanges and recognise that exchanges play a key role in enabling the technological enforcement of the broader governance of a digital ID system.

Chapter 5—Role requirements for accredited entities : identity exchanges

43. Do you have any feedback or suggestions regarding the proposed rules for identity exchanges?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Chapter 6—Annual Reviews

Chapter 6 of the Rules sets out an accredited entity's obligations to conduct and submit an annual review of its ongoing compliance with the Bill and the Rules.

Change from current policy: the Accreditation Rules streamline accredited entity assurance assessment processes. Accredited entities in the pilot accreditation program must submit multiple assurance assessments and extensive additional evidence to demonstrate the entity continues to operate in accordance with the TDIF. The Accreditation Rules ensure the initial accreditation process is more robust than under the current published TDIF. Annual review requirements are then simplified.

The following sections detail the changes to the annual review requirements for accredited entities under the Accreditation Rules.

Review of changes to an entity's DI data environment

Rules 6.1 and **6.2** describe the scope and requirements for an accredited entity to comply with for an annual review. An accredited entity is required to record changes to its DI data environment since the previous annual review and assess whether those changes are a *material change*.

Where the change is a material change, the accredited entity must engage an assessor to conduct an assurance assessment, systems testing or other testing in accordance with the requirements in **Chapter 3** and **Chapter 5, Part 2** of the Rules. The scope of the assurance assessment, systems testing or other testing is only where the material change affects the entities compliance with the requirements of these rules, the details of which the entity must provide to the independent assessor.

Where there are no changes to an entity's DI data environment, an accredited entity is not required to conduct assurance assessments or systems testing apart from those described in **rule 6.3** and **rule 6.4**.

Chapter 6—Annual Reviews : material changes

44. Are there any risks or issues with the proposed rules for material changes assessment during the annual review?

45. Do you have any feedback or suggestions regarding the proposed rules?

If relevant, please provide specific feedback with reference to the Accreditation Rules and a description of how the change would benefit the accreditation scheme.

Change from current policy: The current published TDIF requires the following assurance activities assessment process for annual assessments. An entity must engage an assessor to conduct a:

- PIA if the entity makes a high-risk change to its DI data environment
- privacy assessment against the TDIF PRIV requirements
- penetration test
- security assessment against the TDIF PROT requirements
- WCAG 2.0 or 2.1 test to confirm compliance to the AA standard
- An entity must engage a user researcher to conduct usability testing, if applicable.

Every second year, assessors must be external to the organisation. The regulator is required to assess the entity's compliance against the FRAUD, UX, and TEST requirements and any applicable role-specific requirements located in the *TDIF 07 Maintain accreditation* document.

Please see **Table 1 – Assurance assessment and testing summary** of this document for a simplified explanation of the cadence for assurance assessments and systems testing required under the Rules.

Assurance assessments

Rules 6.3 and **6.4** describes which assurance assessments, systems testing and other testing are required and the cadence.

Regular assurance assessments and systems testing is still required by the new Annual Review rules. This includes yearly penetration testing and fraud and protective security assurance assessments conducted by an independent assessor every 2 years. This is because fraud and protective security are two domains where the risk landscape and malicious attackers are constantly evolving and affecting the continued operations of Digital ID services. This is a change from current policy in the following ways:

- (New) fraud assurance assessment required every 2 years.
  - the fraud assurance assessment must be conducted by an independent assessor except where an accredited entity seeks to meet the requirements of **rule 6.3 (2).**
- (Changed) protective security assurance assessment required every 2 years.
- (Changed) presentation attack detection (PAD) testing required every second year.
  - advice was received from a security expert that the biometric fraud risk and biometric technology landscape is moving so rapidly at this stage that it is recommended that accredited entities utilising online biometric binding in accordance with **rule 5.20** conduct PAD testing on their PAD technology every 2 years. This ensures that the PAD technology is keeping up with developments in fraud attacks that could compromise Digital IDs.

The cadence of the security assurance assessment aligns with the Consumer Data Right annual assessment rules for security assessments. The proposed policy and changes to the protective security rules in **Chapter 4,** including an accredited entity's responsibility to maintain a protective security and fraud capability that manages risks also support this change.

This is because the material changes policy of **rule 6.2** has replaced the need to have an accredited entity constantly conduct assurance assessments or systems testing, which is a costly and time-consuming activity, for their compliance with the Rules where nothing has changed in the DI data environment. Additionally, accredited entities are required to submit an attestation along with any required evidence that they have assessed their continued compliance with the Rules and confirm they continue to comply.