Digital ID (Accreditation) Rules 2024 DRAFT

I, Katy Gallagher, Minister for Finance, make the following rules.

Dated

Katy Gallagher
DRAFT ONLY—NOT FOR SIGNATURE

Minister for Finance

Version 4, 20 May 2024/KLR

Contents

Chapter 1—Preliminary

1.1 Name

These rules are the *Digital ID (Accreditation) Rules 2024 DRAFT*.

1.2 Commencement

(1) Each provision of these rules specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
The whole of this instrument	The time at which the *Digital ID Act 2024* commences.	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

[Consultation note: It is intended that these rules will be in force at the same time as the Act commences and will therefore apply immediately to entities which are taken to be accredited when the Act commences because of the Digital ID (Transitional and Consequential Amendments) Act 2024*. Transitioned accredited entities are being consulted as to whether any transitional arrangements will be necessary when these rules commence.]*

1.3 Authority

These rules are made under section 168 of the *Digital ID Act 2024* for the purposes of that section and the provisions in the Act in which the term 'Accreditation Rules' occurs.

1.4 Definitions

Note: Some expressions used in these rules are defined in the Act, including:

- accredited entity
- accredited attribute service provider
- accredited identity exchange provider
- accredited identity service provider
- accredited service
- attribute
- attribute service provider
- Australia

- Australian Government Digital ID System
- authenticator
- biometric information
- cyber security incident
- digital ID
- digital ID fraud incident
- Digital ID Regulator
- Digital ID Rules
- Digital ID Regulator
- digital ID system
- enforcement body
- entity
- identity exchange provider
- identity service provider
- participating relying party
- personal information
- privacy impact assessment
- relying party
- restricted attribute .

Note 2: Some expressions used in these rules are defined in the Accreditation Data Standards, including:

- approved cryptography
- authentication level
- AL Table
- document liveness
- eIDVT
- eIDVT biometric matching
- in-device biometric capability
- image quality profile
- liveness detection
- look-up secret
- memorised secret
- multi-factor cryptographic device;
- multi-factor cryptographic software;
- multi-factor one-time password device
- out-of-band device
- presentation attack
- presentation attack instrument
- presentation attack instrument species
- public key
- single-factor cryptographic device
- single-factor cryptographic software
- single-factor one-time password device.

(1) Expressions defined in the Accreditation Data Standards have the same meaning in these rules.

(2) In these rules:

accessibility and useability assessment—see rule 3.7.

accountable executive, of an entity, means a senior executive of the entity responsible for the overall management of the entity's DI data environment and accredited services.

accreditation condition—see section 16 of the Act.

Accreditation Data Standards means the *Digital ID (Accreditation) Data Standards 2024*.

acquired image means an image of an individual's face that is used as a sample for biometric matching against the corresponding image from the individual's photo ID.

ACSC means the Australian Cyber Security Centre.

Act means the *Digital ID Act 2024.*

assessing officer means a member of personnel of an accredited entity who is trained and authorised by that entity to conduct local biometric binding or manual face comparison.

assessor—see rule 3.2.

assessor's report—see rule 3.17.

assurance assessment means a protective security assessment, fraud assessment or accessibility and useability assessment—see Part 3.2.

authenticated session means a persistent interaction between two entities involved in a transaction in a digital ID system which begins with an authentication event and ends with an event that brings the authenticated session to an end.

Note: The session could terminate after a specific period, or on the occurrence of a specific event such as the individual closing the browser or logging out.

authentication event means the process of an individual using their authenticator to verify that they are the valid user of a digital ID.

authoritative source means a person that issues documents or other credentials containing information about an individual.

Australian passport has the same meaning as in the *Australian Passports Act 2005*.

biometric binding means the process of confirming the link between an individual and a photo ID by conducting biometric matching for the purpose of obtaining IP level 2 Plus, IP level 3 or IP level 4.

Note: See item 4 of the IP Levels Table.

biometric capability means the components of an accredited entity's DI data environment that process or are involved in the processing of biometric information (including for biometric binding and biometric matching).

biometric matching means one-to-one comparison of an individual against the image on their photo ID.

biometric matching algorithm means the algorithm used to conduct biometric matching.

CoI credential is short for commencement of identity credential.

commencement of identity credential means a document or other credential listed in Schedule 1.

Note: A commencement of identity document evidences an individual's commencement of identity in Australia.

cryptographic key means a string of characters used with approved cryptography to encrypt and decrypt.

cyber security risk means the risk of a cyber security incident occurring in relation to an entity's DI data environment or accredited services.

cyber security risk assessment—see rule 4.7.

data breach means loss or misuse of, unauthorised access to, or unauthorised modification or disclosure of, personal information held by an accredited entity.

DI data environment means the information technology systems used for, and the processes that relate to, the provision of an entity's accredited services or, for an applicant for accreditation, the accredited services the entity proposes to provide.

ePassport means a travel document size 3 machine readable travel document conforming to the specifications of Part 4 of the ICAO Doc 9303 Standard that additionally incorporates a contactless integrated circuit.

fraud assessment—see Division 2 of Part 3.2.

fraud control plan—see rule 4.31

fraud management capability—see rule 4.24.

fraud risk means the risk of a digital ID fraud incident occurring.

fraud risk assessment—see rule 4.25.

hold has the same meaning as in the Privacy Act.

ICAO Doc 9303 Standard means the standard for machine readable travel documents published by the International Civil Aviation Organisation.

Note: At the time these rules were made, located at https://www.icao.int/publications/pages/publication.aspx?docnum=9303

identity proofing means the process to verify an attribute of an individual to generate, manage or maintain the digital ID of the individual.

identity proofing level means a level specified in the first row of the IP Levels Table.

IP level is short for identity proofing level.

IP Levels Table means the table in rule 5.11.

ISM means the Australian Government Information Security Manual published by the ACSC.

Note: At the time these rules were made, located at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism).

linking credential means a document or other credential listed in Schedule 2.

Note: A linking credential demonstrates the continuity of the individual's verified identity where that individual's attributes have changed.

local biometric binding means biometric binding conducted by and in the physical presence of the entity's assessing officer.

manual face comparison means the process of using visual verification to compare the likeness of an individual to the individual's claimed photo ID, conducted by, and in the physical presence of, the entity's assessing officer.

online biometric binding means biometric binding conducted remotely via unsupervised data capture processes conducted across the internet.

personnel, of an entity, means:

(a) an employee of the entity; or

(b) an individual who, under a labour hire, consultancy or similar arrangement with the entity, performs work for the entity in relation to its accredited services.

photo ID means a document listed in Schedule 4.

physical authenticator—see rule 5.27.

Privacy Act means the *Privacy Act 1988*.

protective security assessment—see Division 1 of Part 3.2.

protective security capability—see Division 1 of Part.4.1.

protective security framework—see Division 2 of Part.4.1.

PSPF means the Protective Security Policy Framework published by the Australian Government.

Note 1: At the time these rules were made, located at https://www.protectivesecurity.gov.au/

Note 2: The specific controls in the PSPF to be implemented are listed in Schedule 5.

public-facing accredited services means the accredited services or elements of an entity's information technology system that an individual directly interacts with when using, or attempting to use, the entity's accredited services.

Example: An example of public-facing accredited services is where an individual provides information to be verified via an accredited identity service provider's mobile app that the individual is required to download so as to access the entity's accredited services.

public-facing information related to accredited services means information made available by the accredited entity to individuals when interacting with the entity's public-facing accredited services.

Example: Public-facing information related to accredited services is the accredited entity's privacy policy made available to individuals.

reporting period, for an accredited entity—see rules 6.2 and 6.3.

Note: Chapter 6 requires an accredited entity to conduct an annual review, and report on that review, in each 12-month reporting period.

reusable digital ID means a digital ID verified for multiple uses by binding an authenticator to the digital ID.

risk assessment means the systematic, iterative and collaborative process of identification, analysis and evaluation of risk.

single logout means the ability for an individual to initiate a logout process for relying parties that relied on a single logon session for the individual at an exchange operated by an accredited identity exchange provider.

single sign on means the ability for an individual to make use of their digital ID at multiple services in a short period of time, with a single user authentication.

source biometric matching means the process of using source verification to verify that an acquired image biometrically matches the image on the document or other credential held by the authoritative source.

source verification means the process of verifying an attribute of an individual or a document or other credential in relation to the individual:

(a) with the authoritative source for that attribute or document or other credential; or

(b) through information provided by a service that confirms the veracity of the attribute or document or other credential with an authoritative source.

Note: A service that confirms the veracity of information includes a DVS or FVS (within the meaning of those terms in the *Identity Verification Services Act 2023)*.

special attribute—see rule 5.36 (*verifying and managing a special attribute)*.

Note: An accredited attribute service provider is accredited to verify and manage a special attribute of an individual such as an authorisation for, or qualification of, an individual.

statement of scope and applicability means a statement:

(a) that lists each requirement in these rules and the Accreditation Data Standards with which an entity must comply in relation to its accredited services, or for an applicant, its proposed accredited services; and

(b) the evidence that demonstrates the entity complies with those requirements or, for an applicant, will comply if accredited.

systems testing means penetration testing, useability testing or WCAG testing, each as referred to in Part 3.3.

taking reasonable steps—see rule 1.6.

system security plan—see rule 4.12.

technical biometric matching means the process of verifying that the acquired image of an individual biometrically matches the image on the document or credential, where the document or credential and the image have been verified using technical verification.

technical testing means testing of information technology systems by executing the user flows, user interactions and component interactions.

technical verification means the process of verifying, via public key infrastructure technology, physical or electronic documents or other credentials using approved cryptography.

UitC credential means a document or other credential listed in Schedule 3.

Note: A UitC credential evidences an individual's use in the Australian community of the individual's identity.

visa has the same meaning as in the *Migration Act 1958* and includes an entry permit (within the meaning of that term in the *Migration Act 1958* as in force immediately before 1 September 1994).

visual verification means visually confirming that a document or other credential presented by an individual in-person, and information on that document or other credential, is legitimate.

WCAG means the Web Content Accessibility Guidelines version 2.2 published by the World Wide Web Consortium**.**

Note: At the time these rules were made, located at https://www.w3.org/TR/WCAG21/ . World Wide Web Consortium is commonly known as 'W3C'.

1.5 Incorporated instruments

(1) If a provision of these rules incorporates or applies, with or without modification, matters contained in any other instrument or other writing (***incorporated instrument***), then, unless the contrary intention appears in the provision, the reference to the incorporated instrument is a reference to the incorporated instrument as in force or existing from time to time.

(2) Unless the contrary intention appears in these rules, an accredited entity is not required to comply with a change to an incorporated instrument until 12 months after the change has taken effect for the purposes of the incorporated instrument.

Note: See paragraph 167 of the Act.

(3) Subclause (2) does not apply to the provisions of an Act or a legislative instrument.

1.6 Taking reasonable steps

In these rules, ***taking reasonable steps***, in relation to a duty to ensure an identified outcome, refers to steps that are, or were at a particular time, reasonably able to be done in relation to ensuring that outcome, taking into account and weighing up all relevant matters including:

(a) the likelihood of risks to achievement of the outcome occurring;

(b) the degree of harm that might result if the outcome is not achieved;

(c) what the person who has the duty knows, or ought reasonably to know, about:

(i) the risks to achievement of the outcome; and

(ii) ways of eliminating or minimising the risks;

(d) the availability and suitability of ways to eliminate or minimise the risks; and

(e) after assessing the extent of the risks and the available ways of eliminating or minimising them, the cost associated with available ways of eliminating or minimising the risks, including whether the cost is grossly disproportionate to the risks.

Chapter 2—Applying for accreditation

2.1 DI data environment

For paragraph 15(4)(d) of the Act, the Digital ID Regulator must not accredit an applicant unless the Regulator is satisfied that the entity:

(a) has correctly and completely defined and documented the boundaries of its DI data environment, including:

(i) identifying the people, processes, technology and infrastructure that will manage, secure, store or otherwise interact with the information collected, used, held or disclosed for the purpose of providing its accredited services, if accredited; and

(ii) infrastructure owned by, and management provided by, a contractor engaged, or to be engaged, by the applicant to provide an accredited service, or part of an accredited service, of the applicant if accredited;

(b) has limited the boundaries of its DI data environment to the extent practicable having regard to:

(i) segregation of the environment from other systems;

(ii) minimising the number of people who interact with the information referred to in paragraph (a);

(iii) limiting the number of systems hosting, processing or accessing the information referred to in paragraph (a); and

(iv) minimising the use of contracted service providers interacting with the information referred to in paragraph (a).

2.2 Documents to accompany application

For the purposes of paragraph 141(1)(c) of the Act, an application for accreditation must be accompanied by:

(a) a statement of scope and applicability; and

(b) a statement, signed by the applicant's accountable executive, attesting that:

(i) the technical testing required by rule 2.5 has been conducted;

(ii) the accountable executive is satisfied the results of the technical testing demonstrate that the requirements listed in subrule 2.5(1) will be met if accredited; and

(iii) where a cloud service provider has conducted penetration testing as referred to in paragraph 3.8(4)(a)—the entity is satisfied that that penetration testing covers the kinds of penetration testing in subrule 3.8(2); and

(c) for biometric testing conducted as required by the Accreditation Data Standards, copy of reports of the testing and any responses required to a report.

Note: An approved form for an application may require additional information and documents to be provided (see section 141 of the Act).

2.3 Criteria to be met

(1) An applicant for accreditation must meet the criteria in this rule.

Note: See paragraph 15(4)(c) of the Act.

(2) The applicant must have, at the time it applies for accreditation, an operational information technology system through which it will provide its accredited services if accredited.

(3) The applicant must have conducted:

(a) each kind of assurance assessment;

(b) each kind of systems testing applicable to the accredited services the applicant will provide if accredited;

(c) a privacy impact assessment in accordance with rule 2.4; and

(d) technical testing in accordance with rule 2.5;

(e) if the applicant will conduct biometric binding if accredited—biometric testing in accordance with the Accreditation Data Standards as if references in that instrument to 'ISP' were to 'the applicant'.

Note: See Chapter 3 for assurance assessments and systems testing, and reports to be provided.

2.4 Privacy impact assessment

(1) An applicant must conduct a privacy impact assessment in accordance with this rule.

(2) The privacy impact assessment must:

(a) assess the privacy impacts of:

(i) the applicant's DI data environment and the boundaries of that environment as defined and documented for rule 2.1; and

(ii) the applicant's proposed accredited services;

(b) be conducted by a person who:

(i) has appropriate experience, training and qualifications to conduct a privacy impact assessment;

(ii) is external to the applicant and, if the applicant is part of a corporate group, external to the group; and

(iii) is not, and has not, been involved in the design, implementation, operation or management of the

applicant's accredited services or DI data environment; and

(c) include:

(i) details of the flow of personal information into, within and from the applicant's DI data environment;

(ii) an assessment of the relevant documentation, processes and mechanisms to facilitate the applicant's ability to comply with the privacy requirements specified in Chapter 3 of the Act and Part 3 of Chapter 4 of these rules;

(iii) an analysis of how the applicant's provision of its proposed accredited services, including the requirements in Chapter 5 of these rules and the Accreditation Data Standards as those requirements and standards apply to the proposed accredited services, will impact the privacy of individuals and protection of personal information;

(iv) an analysis as to whether any privacy risks or impacts identified in the privacy impact assessment are necessary or unavoidable;

(v) whether any recommendations of the person who conducted the privacy impact assessment to mitigate any privacy risks or impacts have been accepted and, if not, why treatments to deal with such risks or recommendations are not necessary; and

(vi) details of consultation with relevant stakeholders.

(3) The applicant must respond in writing to the findings of the privacy impact assessment.

(4) The applicant's response to the privacy impact assessment must be signed by the applicant's accountable executive.

(5) For each risk and recommendation identified in the privacy impact assessment, the applicant must:

(a) develop a risk matrix based on an established risk management framework or standard;

(b) conduct a risk assessment;

(c) assign a risk rating in accordance with its risk matrix;

(d) respond to each risk identified in the report as requiring treatment; and

(e) respond to each recommendation in the assessment.

(6) The applicant's response to each risk requiring treatment and each recommendation must include:

(a) for each risk and recommendation accepted by the applicant:

(i) details of the action the applicant will take to implement the treatment or recommendation;

(ii) the timeframe in which the applicant will complete the action, having regard to the risk rating assigned for the risk or recommendation; and

(iii) the residual risk rating expected following completion of the action; and

(b) for each risk and recommendation not accepted by the applicant:

(i) the reasons for the non-acceptance;

(ii) details of alternative actions, if any, to be taken by the applicant; and

(iii) the residual risk rating expected following implementation of any alternative action.

2.5 Technical testing

(1) An applicant must conduct technical testing of its information technology system through which it will provide its accredited services so as to ensure the system has the functionality necessary to meet the following requirements:

(a) incident investigation, management and response for cyber security incidents as required by Subdivision 3 of Part 4.1;

(b) logging requirements as required by rule 4.20;

(c) incident monitoring and detection for fraud incidents as required by Division 4 of Part 4.4;

(d) support to individuals as required by rules 4.11 and 4.30;

(e) data minimisation as required by rule 4.42(2); and

(e) compliance with the Accreditation Data Standards that are specific to the kind of accredited services the applicant will provide if accredited.

(2) The entity must record in respect of the technical testing conducted:

(a) the test completion criteria used;

(b) the assumptions, limitations and dependencies used;

(c) the methodology used, including a description of the data and environment used to conduct the testing;

(d) a requirements traceability matrix which maps the technical testing completed to each requirement referred to in subrule (1); and

(e) the results of the technical testing, including any defects identified and detail of how those defects have been addressed.

2.6 Matters to which the Digital ID Regulator must have regard

For paragraph 15(5)(a) of the Act (matters to which the Digital ID Regulator must have regard when deciding whether to accredit an entity), the following matters are prescribed:

(a) the level of the applicant's tolerance of fraud risks and whether the level is likely to create an unacceptable risk in respect of the accredited services to be provided by the applicant if accredited;

(b) the level of the applicant's tolerance of cyber security risks and whether the level is likely to create an unacceptable risk in respect of the accredited services to be provided by the applicant if accredited; and

(c) whether the applicant's privacy impact assessment and the applicant's response to that assessment identifies any matters that may give rise to an unacceptable risk to the privacy of individuals.

2.7 Matters of which the Digital ID Regulator must be satisfied

For paragraph 15(4)(d) of the Act, the Digital ID Regulator must be satisfied that the information and documents provided by the applicant demonstrate that the applicant, if accredited in accordance with its application, will be able to comply with:

(a) the Act;

(b) these rules; and

(c) the Accreditation Data Standards to the extent a standard relates to a particular activity to be conducted by the entity.

Note: Accredited entities must comply with the Accreditation Data Standards applicable to the accredited service being provided and the manner of providing that service (see subparagraph 5.3(1)(a)(ii)).

Chapter 3—Assurance assessments and systems testing

Part 3.1—General requirements

3.1 Entity's obligation

(1) Where an entity is required by a provision of these rules to conduct an assurance assessment or systems testing, the entity must ensure:

(a) the process for the assurance assessment or systems testing complies with the requirements of this Chapter; and

(b) the assessor assesses that the elements of the DI data environment that are being assessed or tested meet the requirements of the Act and these rules relevant to the kind of assurance assessment or systems testing being conducted.

Note: Applicants are required to conduct assurance assessments and systems testing for their application for accreditation (see subrule 2.3(3)). Accredited entities are required, in accordance with Chapter 6, to conduct assurance assessments and systems testing for annual reviews.

(2) Each assurance assessment and systems testing must be conducted:

(a) having regard to the requirements with which the entity must comply as detailed in the entity's statement of scope and applicability; and

(b) in respect of the applicant's DI data environment,

as at the time the assurance assessment or systems testing is conducted.

3.2 Assessors

(1) An assurance assessment and systems testing must be conducted by an individual:

(a) who has appropriate experience, training and qualifications to conduct that kind of assessment or systems testing; and

(b) if additional requirements relating to the assessor are specified in these rules for that kind of assurance assessment or systems testing—who meets those requirements.

(2) If required by the assessor, an entity must take reasonable steps:

(a) to permit the assessor to have secure online access to documentation and information relevant to the assurance assessment or systems testing; and

(b) to undertake a site visit to the entity's premises or other location at which the accredited services are, or will be, provided.

Part 3.2—Assurance assessments

Division 1—Protective security assessment

3.3 Requirements

(1) A protective security assessment must:
  (a) review and assess the entity's:
    (i) implementation of, and compliance with, the controls in the protective security framework it uses, or will use if accredited;
    (ii) protective security capability;
    (iii) compliance with the additional protective security controls in Division 2 of Part 4.1, or ability to comply if accredited;
  (b) review and address the results of the penetration testing report referred to in rule 3.10;
  (e) review and address findings and any recommendations in the entity's report of its essential strategies review (see paragraph 3.4(2)(b)); and
  (f) where the entity considers a control is not relevant to the entity—comply with the requirements of rule 3.5.

(2) For a protective security assessment involving ISO/IEC 27001, the assessor conducting the assessment must be accredited, or recognised, by the Joint Accreditation System of Australia and New Zealand (JASANZ) to certify entities against ISO/IEC 27001, and must satisfy subrule (3).

(3) For a protective security assessment, the assessor conducting the assessment must, in addition to any requirements relating to assessors in the applicable protective security framework:
  (a) be external to the entity and, if the entity is part of a corporate group, external to the group; and
  (b) not be, or have been, involved in the design, implementation, operation or management of the entity's DI data environment or accredited services.

3.4 Essential strategies review and report

(1) In this rule:

Essential Eight Maturity Model to ISM Mapping document means the document titled 'Essential Eight Maturity Model to ISM Mapping' published by the ACSC.

Note: At the time these rules were made, located at https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20to%20ISM%20Mapping%20%28March%202023%29.pdf.

Essential Eight Assessment Process Guide means the document titled 'Essential Eight Assessment Process Guide' published by the ACSC.

Note: At the time these rules were made, located at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-assessment-process-guide.

(2) An entity must:

(a) review and assess its compliance with rule 4.19 (*Essential Eight*) by conducting an assessment of its implementation and compliance with the Essential Eight Maturity Model to ISM mapping document for ISM controls marked maturity level 2; and

(b) provide a report to the assessor conducting the protective security assessment.

(3) The essential strategies review for subsection (2) must be conducted by a person who has appropriate experience, training and qualifications to conduct the review.

(4) The report of the review must be in the form of the assessment report template in the Essential Eight Assessment Process Guide and must include the following additional information:

(a) the opinion of the person conducting the review as to whether the entity has implemented and complies with maturity level two controls specified in the ISM;

(b) where an entity has implemented an alternative control in place of a control specified in the ISM—a description of that control and its effectiveness at mitigating the relevant cyber security risk; and

(c) findings and recommendations on the entity's essential strategies.

3.5 Where a control is not relevant to an entity

(1) If an entity considers that a particular protective security control is not relevant to the entity, and therefore will not be implemented, the entity must:

(a) give the assessor a risk-based justification for the entity's opinion that the control is not relevant;

(b) give the assessor details of controls or any risk-mitigation strategies taken by the entity to mitigate any residual risk relevant to the control that is not relevant; and

(c) ensure the assessor includes in the report of the assessment, the assessor's opinion as to:

(i) whether the entity's risk-based justification is appropriate and warranted;

(ii) the extent, if any, of residual risk as a result of not implementing the requirement;

(iii) the appropriateness of controls or risk-mitigation strategies taken by the entity to mitigate any cyber security risks that the protective security control is intended to mitigate; and

(iv) whether the protective security control is not relevant to the entity.

Example: A control involving physical security may not be relevant to an entity because the entity's personnel work remotely and the entity does not have a physical office.

(2) If the assessor does not agree that the control is not relevant to the entity, the control must be implemented.

Division 2—Fraud assessment

3.6 Requirement

(1) A fraud assessment must review and assess:

(a) an entity's implementation and compliance with the fraud control requirements in Part 4.2; and

(b) whether the entity's fraud processes are sufficient to respond to emerging risks and threats to its DI data environment.

(2) The assessor conducting the assessment must meet the following additional requirements:

(a) be external to the entity and, if the entity is part of a corporate group, external to the group; and

(b) not be, or have been, involved in the design, implementation, operation or management of the entity's DI data environment or accredited services.

Division 3—Accessibility and useability assessment

3.7 Requirements

(1) This Division applies for the purposes of subsection 30(1) and paragraphs 30(2)(a) to (c) of the Act (*Accredited services must be accessible and inclusive*).

(2) An accessibility and useability assessment must review and assess:
   (a) the entity's implementation and compliance with rule 4.50;
   (b) for an accredited identity service provider—the entity's implementation and compliance with the additional accessibility and useability requirements in Division 3 of Part 5.2 (*Accessibility and useability*);
   (c) the findings of the WCAG testing, including treatments that will address any risks and recommendations identified in the assessor's report of the WCAG testing; and
   (d) where the entity is required to conduct useability testing—the findings of the useability testing, including treatments that will address any risks and recommendations identified in the assessor's report of the useability testing.

Part 3.3—Systems testing

Division 1—Penetration testing

3.8 Penetration testing requirements

(1) Penetration testing must evaluate the effectiveness of the implementation of security controls in the information technology system through which the entity provides, or will provide, its accredited services by emulating the tools and techniques of likely attackers to exploit security weaknesses.

(2) The penetration testing must include:
  (a) testing of egress and ingress points of the information technology system;
  (b) non-authenticated penetration testing (also known as black-box testing); and
  (c) authenticated penetration testing (also known as white-box testing).

(3) Where an entity uses infrastructure of a cloud service provider as part of its information technology system within its DI data environment, the penetration testing required by subrule (2) is required to be conducted only on that part of the entity's information technology system that is hosted by, or part of the tenancy with, the cloud service provider (***cloud service provider's infrastructure***).

(4) However, if an entity's arrangement with a cloud service provider does not allow penetration testing by the entity of the cloud service provider's infrastructure:
  (a) an applicant must ensure the cloud service provider has conducted on that infrastructure the kinds of penetration testing referred to in subrule (2);
  (b) an accredited entity must ensure the cloud service provider, at least once in each of the accredited entity's reporting periods, conducts on that infrastructure the kinds of penetration testing referred to in subrule (2); and
  (c) the other requirements in this Part relating to penetration testing do not apply to the penetration testing conducted by the cloud service provider.

(3) The penetration testing by the accredited entity's assessor must be conducted before the protective security assessment.

Rule 3.9

3.9 Penetration testing assessor

The assessor conducting the penetration testing must meet the following additional requirements:

(a) be external to the entity and, if the entity is part of a corporate group, external to the group; and

(b) not be, or have been, involved in the design, implementation, operation or management of the entity's DI data environment or accredited services.

3.10 Penetration testing report

The assessor must prepare a testing report that includes:

(a) a description of the tools and processes used to conduct penetration testing;

(b) a description of the scope of the penetration testing; and

(c) the test results, including:

(i) any findings, including identification of any security risks or vulnerabilities to the entity's DI data environment, including to its information technology system when in operation; and

(ii) any recommendations.

Division 2—Useability testing

3.11 Accessible and inclusive services

This Division applies for the purposes of section 30(1) of the Act (*Accredited services must be accessible and inclusive*).

3.12 Useability testing requirements

(1) Useability testing of an entity's public-facing accredited services must:
  (a) identify issues in the design, useability and accessibility of the entity's public-facing accredited services; and
  (b) if any adverse issues relating to useability and accessibility by individuals are identified by the assessment, make recommendations on improvements to the entity's public-facing accredited services to address those issues and to reduce or mitigate any useability issues identified.

(2) The useability testing must:
  (a) cover the end-to-end user journey as detailed in the user journey map required by rule 4.51;
  (b) for the purposes of section paragraph 30(2)(c) of the Act—involve a diverse range of individuals covering diversity in disability, age, gender and ethnicity; and
  (c) for the purposes of paragraph 30(2)(d) of the Act—involve a wide range of devices, browser access and platforms so that the testing demonstrates a continuity of support for access to the accredited services across those devices, browsers and platforms.

3.13 Useability testing report

The assessor must prepare a testing report that includes:
  (a) a description of the tools and processes used to conduct the testing; and
  (b) a description of the scope of testing to cover:
    (i) findings and quantitative metrics; and
    (ii) identification of user issues and recommendations to address accessibility and useability involving the entity's accredited services.

Division 3—WCAG testing

3.14 Accessible and inclusive services

This Division applies for the purposes of paragraph 30(1) of the Act (*Accredited services must be accessible and inclusive*).

3.15 WCAG testing requirements

WCAG testing must test the extent to which the entity's public-facing accredited services and public-facing information related to its accredited services meet WCAG version 2.1 to Level A conformance and Level AA conformance within the meaning of those terms in the WCAG (see Part 4.4 (*Accessible and inclusive accredited services*)).

3.16 WCAG testing report

The assessor must prepare a WCAG testing report that includes:

(a) description of the entity's public-facing accredited services and public-facing information related to its accredited services that were tested;

(b) a description of the tools and processes used to test WCAG compliance; and

(c) the testing results, including:

(i) any findings and recommendations; and

(ii) identification of any risks to accessibility by individuals when the entity's information technology system is in operation.

Part 3.4—Reports for assurance assessments and systems testing

3.17 Assessor's report

For each kind of assurance assessment and systems testing, the assessor must prepare a report (***assessor's report)*** for that assessment or testing that includes, the following:

(a) a summary of the activities, including any site visits and interviews, undertaken by the assessor when conducting the assurance assessment or systems testing;

(b) the dates on which the assurance assessment or systems testing was commenced and completed;

(c) details of the qualifications and experience of the assessor;

(d) details of the release number or version number of the information technology system being assessed;

(e) a description and version number of each document considered by the assessor;

(f) the evaluation or test methodology used; and

(g) the findings of the assurance assessment or systems testing, including:

(i) details of any non-compliance with the Act, these rules and applicable Accreditation Data Standards relevant to the assurance assessment and systems testing;

(ii) details of any risks identified by the assessor and any treatment to remove or mitigate the risk; and

(iii) any recommendations to the entity to treat any risks or to ensure compliance with the Act and these rules relevant to the assurance assessment and systems testing.

3.18 Entity's response to an assessor's report

(1) An entity must respond in writing to the findings of each assessor's report (***entity's response***) as required by this rule.

(2) The entity's response to an assessor's report must be signed by the entity's accountable executive.

(3) For each risk and recommendation identified in an assessor's report, the entity must:

(a) develop a risk matrix based on an established risk management framework;

(b) conduct a risk assessment;

(c) assign a risk rating in accordance with its risk matrix;

(d) respond to each risk identified in the report which requires treatment to contain or mitigate the risk; and

(e) respond to each recommendation in the report.

(2) The entity's response to each risk requiring treatment and each recommendation must include:

(a) for each risk and recommendation accepted by the entity:

(i) details of the action the entity will take to implement the treatment or recommendation;

(ii) the timeframe in which the entity will complete the action, having regard to the risk rating assigned for the risk or recommendation; and

(iii) the residual risk rating expected following completion of the action; and

(b) for each risk and recommendation not accepted by the entity:

(i) the reasons for the non-acceptance;

(ii) details of alternative actions, if any, to be taken by the entity and the timeframes to do so; and

(iii) the residual risk rating expected following implementation of any alternative action.

Chapter 4—Requirements for maintaining accreditation

Part 4.1—Protective security controls

Division 1—Capability

4.1 Protective security capability

(1) ***Protective security capability*** of an accredited entity means the accredited entity's ability to manage protective security of its DI data environment in practice through the implementation and operation of processes and controls, including by:
  (a) allocating adequate budget and resources; and
  (b) providing for management oversight.

(2) An accredited entity's protective security capability must be appropriate and adapted to respond to cyber security risks, including emerging risks, having regard to:
  (a) the extent and nature of the personal information the entity holds;
  (b) the extent and nature of cyber security risks, threats and vulnerabilities;
  (c) the potential loss or damage to one or more individuals if a cyber security incident were to occur;
  (d) the potential loss or damage to relying parties if a cyber security incident were to occur; and
  (e) the potential loss or damage to entities and individuals if a cyber security incident were to occur and result in a digital ID being compromised or otherwise rendered unreliable.

(3) An accredited entity must take reasonable steps to prevent, detect and deal with cyber security incidents, including by:
  (a) having and maintaining a protective security capability;
  (b) continuously improving its protective security capability; and
  (c) identifying, treating and managing cyber security risks.

Division 2—Protective security frameworks

4.2 Accredited entities must implement a security framework

(1) An accredited entity must implement, in respect of its accredited services and DI data environment, one of the following:
  (a) the PSPF;
  (b) ISO/IEC 27001; or
  (c) subject to the requirements in rule 4.5—an alternative framework.

4.3 Compliance with the PSPF

(1) An accredited entity that implements the PSPF must comply with, and manage and monitor, each of the controls in that framework that are listed in Schedule 5 as follows:
  (a) the controls listed in the column headed 'B.2 Supporting requirement;
  (b) the controls listed in the column headed 'Requirement'; and
  (c) the controls listed in the column headed 'Sub-requirement'.

(2) Subrule (1) applies subject to rule 4.6 (*Where a control is not relevant to an entity*).

(3) For the purposes of these rules, references to the following terms in the PSPF have the corresponding meanings below:
  (a) 'sensitive information'—the corresponding meaning is 'personal information';
  (b) 'Australian Government resources'—the corresponding meaning is 'DI data environment'.
  (c) 'risks'—the corresponding meaning is 'cyber security risks'.

4.4 Compliance with ISO/IEC 27001

(1) An accredited entity that implements ISO/IEC 27001 must:
  (a) comply with, and manage and monitor, all the controls specified in that standard; and
  (b) if the entity has implemented ISO/IEC 27001: 2013—be compliant with ISO/IEC 27001: 2022 from 31 December 2024.

(2) Subrule (1) applies subject to rule 4.6 (*Where a control is not relevant to an entity*).

(3) For the purposes of these rules, the following terms in ISO/IEC 27001 have the corresponding meanings below:

‘ (a) Personally Identifiable Information’—the corresponding meaning is ‘personal information’;
(b) ‘information security incident’—the corresponding meaning is ‘cyber security incident’;
(c) ‘information security risk’—the corresponding meaning is ‘cyber security risk’.

4.5 Implementation and compliance with an alternative framework

(1) An accredited entity may implement an alternative framework only if the entity demonstrates, in accordance with subrule (2), that the alternative framework covers, and requires compliance with, the same kinds of controls:
(a) in ISO/IEC 27001; or
(b) in the PSPF that would apply to the accredited entity if it implemented the PSPF.

(2) To demonstrate that the alternative framework covers the same kinds of controls, and requires compliance with those controls, the accredited entity must prepare, and maintain an up-to-date document, that maps the controls that must be complied with against:
(a) the corresponding controls in ISO/IEC 27001; or
(b) the corresponding controls in the PSPF as listed in Schedule 5.

(3) An accredited entity that implements an alternative framework must:
(a) comply with, and manage and monitor, all the controls specified in that framework that are mapped to a corresponding control in ISO/IEC 27001 or the PSPF, as the case may be;
(b) comply with a new version of the framework within the timeframe specified for that version.

(4) Subrule (1) applies subject to rule 4.6 (*Where a control is not relevant to an entity*).

4.6 Where a control is not relevant to an entity

An accredited entity is not required to comply with a particular control in the framework it implements if the most recent report of the assessor conducting the protective security assessment for the entity includes the assessor’s opinion that the control is not relevant to the entity because of the entity’s particular circumstances.

Note: See rule 3.5 about an assessor’s opinion that a control is not relevant to an entity.

Example: A control about managing a cloud service provider will not be relevant to an entity if the entity does not use a cloud service provider when providing its accredited services.

Division 3—Additional protective security controls

4.7 Cyber security risk assessment

(1) An accredited entity must for each reporting period, conduct an assessment of the cyber security risks associated with its accredited services and DI data environment (***cyber security risk assessment***).

(2) An accredited entity must:
  (a) develop a risk matrix based on an established risk management framework; and
  (b) for the cyber security risk assessment:
    (i) assess the entity's cyber security risks in accordance with the entity's risk matrix;
    (ii) record the results of the assessment;
    (iii) determine and record the entity's level of tolerance to cyber security risks; and
    (iv) record the entity's controls for cyber security risks.

(3) Where an accredited entity collects, uses, holds, discloses or destroys biometric information, the accredited entity must assess and record in its cyber security risk assessment the security risks, mitigation strategies and treatments related to biometric information.

4.8 Sharing information about risks

An accredited entity must:
  (a) consider the implications that the entity's decisions related to the management of cyber security risks have for other participants of the digital ID system in which the accredited entity operates; and
  (b) share information on known cyber security risks or cyber security incidents with those participants where appropriate.

4.9 Eligibility and suitability of personnel

An accredited entity must take reasonable steps to ensure the ongoing eligibility and suitability of its personnel who interact with its DI data environment.

Note: If the entity implements the PSPF, this rule may be met by the entity complying with the requirements in PSPF Policy 13.

4.10 Advice to individuals

(1) An accredited identity service provider must provide advice to individuals about how to safeguard their digital ID against cyber security risks and update that advice as risks and threats emerge.

(2) If an accredited entity is aware of a cyber security risk or cyber security incident in the digital ID system in which it operates and which is likely to cause serious harm to an individual, the entity must promptly after becoming aware of the risk or incident:

(a) where individuals interact directly with the entity's public facing accredited services—provide information to individuals as to how to protect themselves from such risks or incidents; or

(b) where individuals do not interact directly with the entity's public facing accredited services—take reasonable steps to notify other participants in the same digital ID system of the incident or risk.

Example: An individual not interacting directly with an entity's accredited services includes where the individual interacts only with the relying party or another third-party during verification or authentication related to the individual.

4.11 Support to individuals

(1) An accredited entity with public-facing accredited services must provide support to individuals who have been adversely affected by a cyber security incident.

(2) Support services must include, at a minimum, the provision of:

(a) a monitored chat or email function; and

(b) a function that allows the individual to speak with a real person.

Subdivision 1—System security plan

4.12 Requirements for system security plan

(1) An accredited entity must have, maintain and comply with a system security plan that meets the requirements of this Subdivision.

(2) If an accredited entity implements ISO/IEC 27001—the entity's system security plan must include:

(a) all documents and processes referred to in ISO/IEC 27001 which together comprise the entity's 'information security management system' within the meaning of that term in ISO/IEC 27001; and

(b) any other information required by these rules to be in the system security plan.

(3) If an accredited entity implements the PSPF—the entity's system security plan for these rules:
(a) is the security plan referred to in PSPF Policy 11; and
(b) must contain any other information required by these rules to be in the system security plan.

Goals and strategic objectives

(4) The entity's system security plan must include details of the entity's:
(a) goals and the strategic objectives to manage and improve its protective security capability; and
(b) activities to continuously improve that capability.

Destruction of biometric information

(5) Where an accredited identity service provider collects biometric information, the entity's system security plan must include details of the processes, procedures and timeframes for the destruction of that biometric information, including destruction of all copies and caches of that information.

(6) Where another person collects biometric information from, or on behalf of, an accredited identity service provider, the accredited identity service provider's system security plan must include details of the arrangements in place for the other entity to destroy that biometric information, including all copies and caches of that information, in accordance with the same timeframes for destruction of biometric information that apply to the accredited identity service provider.

Assessment of risks related to biometric information

(7) Where an accredited identity service provider collects, uses, holds, discloses or destroys biometric information—the system security plan must include details of cyber security risks, and associated mitigation strategies and treatments, related to that biometric information, conducting biometric binding, or authentication using biometric information, including risks relating to:
(a) using biometric matching algorithms to complete biometric binding;
(b) systems for presentation attack detection to complete presentation attack detection;
(c) the capture, temporary storage, and destruction of biometric information;
(d) the biometric matching process the entity implements; and

(e) potential and known threats and attacks to the entity's biometric capability;

Use of out-of-band authenticators via PSTN

(8) Where an accredited identity service provider authenticates an individual by use of an out-of-band device via the public switched telephone network (***PSTN***), the entity must detail in its system security plan:

(a) the risks of using the PSTN, including, but not limited to, risks associated with device swap, SIM change, number porting or other abnormal behaviour; and

(b) risk-management strategies that the entity will implement to ensure those risks will be managed.

4.13 Review of the system security plan

(1) An accredited entity must review and update its system security plan:

(a) at least once in every reporting period; and

(b) as soon as practicable after:

(i) the entity becomes aware of a cyber security incident which is of a kind not covered in the entity's system security plan or which exceeds the entity's recorded level of tolerance of cyber security risks;

(ii) the entity becomes aware of a breach of a requirement specified in its system security plan; or

(iii) a change in the entity's organisational structure or control, functions or activities, where such change will, or is reasonably likely to, increase the level of cyber security risk.

(2) The review of the system security plan for a reporting period must, at a minimum:

(a) have regard to significant shifts in the entity's cyber security risk, threat and operating environment;

(b) include an assessment of the appropriateness of the existing protective cyber security control measures and mitigation controls; and

(c) review and, where necessary, update the goals and strategic objectives in its system security plan, including:

(i) record whether each goal and strategic objective has been met; and

(ii) update the goals and strategic objectives for the next year.

Note: If the entity implements the ISO27001, subrule (2) would be met by the entity complying with clauses 8, 9 and 10 of ISO/IEC 27001.

(3) As soon as practicable after each review, an accredited entity must make all necessary amendments to its system security plan.

Subdivision 2—Cloud service management

4.14 Selection, use and management of cloud services

(1) Where an accredited entity uses cloud services as part of its DI data environment, it must have and maintain a cloud services management plan that includes policies and processes for:
   (a) the selection, use, and management of cloud services;
   (b) defining and recording all relevant protective security requirements associated with the entity's use of cloud services;
   (c) periodic security testing and assessment of assurance for the effective operation of relevant protective security requirements associated with the cloud services provider, including in relation to geographic location, management of privileged access and effective destruction of data;
   (d) responding to cyber security incidents or suspected cyber security incidents involving the cloud services provider;
   (e) the orderly migration of services and information from the cloud services provider;
   (f) the approach to monitoring, reviewing and evaluating the ongoing use of cloud services to manage cyber security risks;
   (g) whether personal information is to be collected, held, used or disclosed by the cloud service provider;
   (h) how personal information is destroyed once it is no longer required; and
   (i) amending or discontinuing the use of cloud services, including exit strategies for cloud services.

(2) An accredited entity must have and maintain a register of cloud service providers which includes the following information:
   (a) cloud services provider's name and cloud service name;
   (b) purpose for using the cloud services;
   (c) the type of personal information collected, used, held or disclosed by the cloud services provider;
   (d) date for the next protective security assurance assessment of the cloud services;
   (e) contractual arrangements for the cloud service; and
   (f) contact details for the cloud service provider, including emergency contact details.

Note: If the entity implements ISO/IEC 27001, this rule would be met by the entity complying with clause 5.23 of Annex A of ISO/IEC 27001.

Subdivision 3—Incident detection, investigation, response and reporting

4.15 Incident monitoring and detection

(1) An accredited entity must implement and maintain appropriate mechanisms for:
  (a) preventing and detecting actual and suspected cyber security incidents; and
  (b) alerting the entity's personnel to actual or suspected cyber security incidents.

(2) Without limiting subrule (1), the mechanisms must include an accessible process for personnel, individuals, enforcement bodies and other relevant entities to report actual or suspected cyber security incidents on a confidential basis.

4.16 Incident investigation, management and response

(1) An accredited entity must implement and maintain mechanisms for investigating or otherwise dealing with cyber security incidents in relation to the accredited entity's DI data environment.

(2) An accredited entity must investigate cyber security incidents and suspected cyber security incidents unless the incident or suspected incident has been referred to, and has been accepted by, the ACSC or an enforcement body.

(3) Without limiting subrule (1), the mechanisms must include processes and procedures to:
  (a) manage and respond to cyber security incidents and suspected cyber security incidents; and
  (b) for an accredited identity service provider:
    (i) identify a digital ID that has been affected by a cyber security incident; and
    (ii) suspend or prevent use of the digital ID; and
  (c) for an accredited attribute service provider:
    (i) identify special attributes that have been affected by a cyber security incident; and
    (ii) suspend or prevent use of the special attribute.

4.17 Disaster recovery and business continuity management

(1) An accredited entity must have, maintain and comply with a disaster recovery and business continuity plan for its DI data environment that covers:
  (a) business continuity governance;
  (b) training requirements for recovery team members;

(c) recovery objectives and priorities;
(d) backup retention and protection from loss processes;
(e) backup recovery and restoration processes;
(f) continuity strategies; and
(g) testing requirements for restoration procedures.

(2) The disaster recovery and business continuity plan for the accredited entity's DI data environment must be separate from its plan in respect of its other business or organisational functions.

(3) An accredited entity, at least once in each reporting period, review and test its disaster recovery and business continuity plan.

Note: If the entity implements ISO/IEC 27001, this rule would be met by the entity complying with clauses 5.30 and 8.13 of ISO/IEC 27001.

4.18 Record keeping

An accredited entity must prepare and keep records of:
(a) decisions to use civil, administrative or disciplinary procedures, or to take no further action, in response to a cyber security incident; and
(b) the entity's investigations of and responses to cyber security incidents that cause, or are likely to cause, serious harm to one or more individuals.

Subdivision 4—Information technology system controls

4.19 Essential Eight

An accredited entity must, in relation to its DI data environment, implement and comply with the mitigation strategies whose 'relative security effectiveness rating' is marked 'essential' in the *Strategies to Mitigate Cyber Security Incidents document* published by the ACSC.

Note: At the time these rules were made, located at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents.

4.20 Logging requirements

(1) An accredited entity's information technology system through which it provides its accredited services must generate logs that record activities, exceptions, faults and events in the entity's DI data environment.

(2) Without limiting subrule (1), the activities to be recorded must include:

(a) the creation, update, use, disclosure and destruction of personal information;
(b) the destruction of biometric information if collected or retained by or on behalf of the accredited identity service provider;
(c) successful and failed elevation of access privileges by personnel;
(d) personnel and group additions, deletions and modification to permissions;
(e) system alerts and failures related to cyber security risks; and
(f) unauthorised attempts to access critical systems and files.

Logging implementation and monitoring plan

(3) An accredited entity must have, maintain and comply with a logging implementation and monitoring plan that details:
(a) how the entity provides, stores, protects, monitors and analyses logs;
(b) how the entity monitors logs for anomalous behaviour; and
(c) the activities, exceptions, faults and other relevant events in the entity's DI data environment.

(4) The logging implementation and monitoring plan must be adapted and appropriate to manage cyber security risks to the entity's accredited services and DI data environment.

(5) Each log required to be generated by this rule must include the following details for each event:
(a) interaction type;
(b) transaction audit identifier;
(c) the names of the entities involved in the event;
(d) any unique identifier used in the event;
(e) for an accredited identity exchange provider—each kind of attribute conveyed for the event;
(f) for accredited entities other than an accredited identity exchange provider—the types of attributes requested and disclosed to each entity involved in the event; and
(g) where the interaction type is of a kind that requires express consent—the audit log for that interaction must include the following as relevant to the interaction:
(i) the date and method by which express consent was obtained from the individual;
(ii) the duration of the express consent;
(iii) whether the express consent was granted, declined or withdrawn by the individual;
(iv) whether the express consent has expired.

Note: If the entity implements ISO/IEC 27001, subrules (1), (3) and (4) would be met by the entity complying with clauses 8.15, 8.16 and 8.17 of Annex A of ISO/IEC 27001.

(6) Subject to clause (6A), a log required by this rule must:
  (a) be retained for a minimum of 3 years from the date it was generated; and
  (b) not contain biometric information.

(6A) The accredited entity must not destroy or de identify information in the possession or control of the entity if:
  (a) the information is personal information; and
  (b) the information was obtained by the entity when providing its accredited services; and
  (c) the entity is required or authorised to retain the information by or under:
    (i) the Act, these rules or the Digital ID Rules;
    (ii) a direction issued by the Digital ID Regulator under section 127 of the Act; or
    (iii) a court/tribunal order (within the meaning of the Privacy Act); and
  (d) the information relates to any current or anticipated legal proceedings or dispute resolution proceedings to which the entity is a party.

(7) A log required by this rule must include a record of:

Accredited identity service providers
  (a) for an accredited identity service provider—the binding of attributes to a digital ID;
  (b) for an accredited identity service provider that provides reusable digital IDs:
    (i) information required to implement and support rate limiting (see the Accreditation Data Standards);
    (ii) the date and time the authenticator was bound to the individual's digital ID;
    (iii) the unique identifier assigned to an individual within the digital ID system in which the entity operates;
    (iv) details of any physical authenticators bound to the digital ID of the individual; and
    (v) details of the source of any unsuccessful authentications attempted with the authenticator;
  (c) for an accredited identity service provider conducting biometric binding—information associated with each biometric binding transaction, including the method of biometric binding used in the transaction; and
  (d) for an accredited identity service provider conducting manual face comparison activities:

(i) the manual face comparison activities conducted during the biometric binding process;
(ii) the assessing officer responsible for conducting any activities related to the biometric binding transaction; and
(iii) whether or not technical verification of the claimed photo ID was completed as part of the biometric binding transaction.

Accredited attribute service providers

(e) for an accredited attribute service provider:
(i) the binding of a special attribute to a digital ID; and
(ii) the retrieval of a special attribute by a third party; and

Accredited identity exchange providers

(f) for an accredited identity exchange provider:
(i) where the accredited identity exchange provider records consent on behalf of an identity service provider or attribute service provider, the duration of consent (including any time limit on the consent); and
(ii) the status of the consent provided by the individual such as 'grant', 'deny' or 'ongoing'.

4.21 Cryptography

An accredited entity must ensure 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.

4.22 Cryptographic standards

(1) An accredited entity must comply with Transport Layer Security 1.3 (***TLS 1.3***) (within the meaning of the term in the ISM).

Note: The cryptographic standards in the ISM include a requirement to implement the latest version of TLS. At the time these rules were made, the current version of TLS is version 1.3.

(2) However, if the entity is unable to comply with TLS 1.3, in relation to an individual, because TLS 1.3 is not supported by the individual's device, the entity must:
(a) implement at least TLS version 1.2; and
(b) follow relevant risk mitigation advice in the document titled *Implementing Certificates, TLS, HTTPS and Opportunistic TLS* published by the ACSC.

Note: At the time these rules were made, located at https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-

Rule 4.23

%20Implementing%20Certificates%2C%20TLS%2C%20HTTPS%20and%20Opportunistic%20TLS%20%28October%202021%29.pdf

4.23 Cryptographic key management processes and procedures

An accredited entity must develop, implement and maintain documented, effective and secure cryptographic key management processes and procedures for its information technology system and which cover cryptographic key lifecycle management, including:

(a) cryptographic key generation;
(b) registration;
(c) distribution;
(d) installation;
(e) usage;
(f) protection;
(g) storage;
(h) access;
(i) revocation;
(j) recovery; and
(k) destruction.

Note: If the entity implements ISO/IEC 27001, this rule would be met by the entity complying with clause 8.24 of Annex A of ISO/IEC 27001.

Part 4.2—Fraud control requirements

Division 1—Capability

4.24 Fraud management capability

(1) ***Fraud management capability*** of an accredited entity means the accredited entity's ability to manage fraud in relation to its accredited services and DI data environment in practice through the implementation and operation of processes and controls, including by:
   (a) allocating adequate budget and resources; and
   (b) providing for management oversight.

(2) An accredited entity's fraud management capability must be appropriate and adapted to respond to fraud risks, having regard to:
   (a) the extent and nature of personal information that the entity holds;
   (b) the extent and nature of fraud risks, threats and vulnerabilities;
   (c) the potential loss or damage to one or more individuals if a digital ID fraud incident occurs;
   (d) the potential loss or damage to relying parties if a digital ID fraud incident occurs; and
   (e) the potential loss or damage to entities and individuals if a digital ID fraud incident occurs that results in a digital ID being compromised or otherwise rendered unreliable.

(4) An accredited entity must take reasonable steps to prevent, detect and deal with digital ID fraud incidents, including by:
   (a) having and maintaining a fraud management capability;
   (b) continuously improving its fraud management capability; and
   (c) identifying, treating and managing fraud risks.

Division 2—Fraud controls

4.25 Fraud risk assessment

(1) An accredited entity must conduct at least once in each reporting period an assessment of the fraud risks associated with its accredited services and DI data environment (***fraud risk assessment***).

(2) The accredited entity must:
  (a) develop a risk matrix based on an established risk-management framework; and
  (b) as part of the fraud risk assessment:
    (a) assess the entity's fraud risks in accordance with the entity's risk matrix;
    (b) record the results of the assessment;
    (c) determine and record the entity's level of tolerance to fraud risks; and
    (d) record how the entity's controls for fraud risks are applied to its accredited services and DI data environment.

(3) Where an accredited identity service provider collects, uses, holds, discloses or destroys biometric information, the entity must assess and record in its fraud risk assessment the fraud risks, mitigation strategies and treatments related to biometric information.

4.26 Sharing information about risks

An accredited entity must:
  (a) consider the implications that the entity's decisions related to the management of fraud risks have for other participants of the digital ID system in which the accredited entity operates; and
  (b) share information on known fraud risks or digital ID fraud incidents with those participants where appropriate.

4.27 Fraud controller

(1) An accredited entity must have a key position of fraud controller held by a senior officer of the entity and who is given responsibility for:
  (a) managing fraud risks; and
  (b) facilitating the entity's compliance with the fraud control requirements specified in this Part.

(2) The fraud controller must have appropriate qualifications and experience to effectively carry out the duties specified for the position in this Part and the entity's fraud control plan.

(3) Details of the fraud controller must be included in the accredited entity's fraud control plan.

4.28 Fraud awareness training

An accredited entity must ensure its personnel whose duties relate to its accredited services or DI data environment successfully complete appropriate training in relation to the management of fraud risks:

(a) before starting work on those duties; and

(b) at least once in every 12-month period thereafter.

4.29 Advice to individuals

(1) An accredited identity service provider must ensure that advice is provided to individuals about how to safeguard their digital ID against fraud risks and update that advice as risks and threats emerge.

(2) If an accredited entity is aware of a fraud risk or digital ID fraud incident in the digital ID system in which it operates and which is likely cause serious harm to an individual, the entity must promptly after becoming aware of the risk or incident:

(a) where individuals interact directly with the entity's public facing accredited services, provide clear and accessible information to individuals about how to protect themselves from such risks or incidents; and

(b) where individuals do not interact directly with the entity's public facing accredited services—take reasonable steps to notify other participants in the same digital ID system of the incident or risk.

Example: An individual not interacting directly with an entity's accredited services includes where the individual interacts only with the relying party or another third-party during verification or authentication related to the individual.

4.30 Support to individuals

(1) An accredited entity with public-facing accredited services must provide support services to individuals who have been adversely affected by a digital ID fraud incident.

(2) Support services must include, at a minimum, the provision of:

(a) a monitored chat or email function; and

(b) a function that allows the individual to speak with a real person.

Division 3—Fraud control plan

4.31 Fraud control plan

(1) An accredited entity must have, maintain and comply with a fraud control plan that details the entity's key fraud risks and the structures, controls and strategies in place to counter fraud in relation to its accredited services and DI data environment.

(2) The fraud control plan must, at a minimum, detail each of the following:

Risks

(a) the fraud risks, threats and vulnerabilities, including fraud risks eventuating through other entities interacting with the entity's DI data environment, that may impact the entity's DI data environment;

(b) an assessment of the significance of the risks, threats and vulnerabilities;

(c) the strategies and controls the entity uses, and proposes to use, to manage fraud risks, threats and vulnerabilities identified for paragraph (a), including strategies and controls to implement and maintain a positive fraud risk culture;

(d) the entity's level of tolerance of fraud risks;

(e) the risk ratings and scale to be used by the entity when assessing the severity of a digital ID fraud incident;

(f) the entity's key positions with responsibility for managing fraud risks and the duties for such positions;

Goals and strategic objectives

(g) the entity's goals and the strategic objectives to manage and improve its fraud management capability;

(h) the entity's proposed steps to continuously improve that capability;

Personnel and training

(i) the strategies and controls to ensure the entity's personnel whose duties relate to the entity's DI data environment successfully complete appropriate training in relation to the prevention and management of fraud risks;

Digital ID fraud incident management

(j) the strategies and controls for managing and investigating digital ID fraud incidents and reporting digital ID fraud incidents to the Digital ID Regulator;

Destruction of biometric information

(k) where an accredited entity collects biometric information, the processes and procedures for the destruction of that biometric information held by or on behalf of the entity, including destruction of all copies and caches;

(l) where another person collects biometric information from, or on behalf of, an accredited identity service provider, the accredited identity service provider's fraud control plan must include details of the arrangements in place for the other entity to destroy that biometric information, including all copies and caches of that information, in accordance with the same timeframes for destruction of biometric information that apply to the accredited identity service provider;

Biometric binding

(m) where an accredited identity service provider conducts biometric binding:

(i) details of the entity's approach to the use of biometric information for fraud-related activities;

(ii) details of the procedures implemented to detect any fraudulent activities by assessing officers when those officers are conducting manual face comparison;

(iii) a description of each location at which the entity will undertake biometric binding; and

(v) the risks, threats and vulnerabilities specific to the use of eIDVT (if used); and

(vi) processes and procedures to ensure the destruction of acquired images of processed photo IDs; and

(vii) the process undertaken to meet the requirements in items 1 to 9 in the IP Levels Table relevant to the identity proofing levels the accredited entity is accredited to provide; and

In-device biometric capability

(n) where an accredited identity service provider conducts authentication using in-device biometric capability—the risks, threats and vulnerabilities specific to the entity's use of in-device biometric capability.

Assessment of risks related to biometric information

(3) Where an accredited entity collects, uses, holds, discloses or destroys biometric information, the fraud control plan must also include details of digital ID fraud risks and associated mitigation strategies and treatments related to that biometric information and to conducting biometric binding or using biometric information for authentication, including risks relating to:

(a) using biometric matching algorithms to complete biometric binding;
(b) using systems for presentation attack detection to complete presentation attack detection;
(c) the capture, temporary storage, and destruction of biometric information;
(d) the biometric matching process the entity implements;
(e) potential and known threats and attacks to the entity's biometric capability; and
(f) using manual processes conducted by assessing officers to complete local biometric binding.

4.32 Review of entity's fraud control plan

(4) An accredited entity must review and update its fraud control plan:
  (a) at least once in every reporting period; and
  (b) as soon as practicable after:
    (i) the entity becomes aware of a digital ID fraud incident which is of a kind not covered in the entity's fraud control plan or which exceeds the entity's recorded level of tolerance of fraud risks; and
    (ii) the entity becomes aware of a breach of a requirement specified in its fraud control plan; and
    (iii) a change in the entity's organisational structure or control, functions or activities, where such change will, or is reasonably likely to, increase fraud risks to the entity's accredited services or DI data environment.

(5) The entity's review of its fraud control plan must, at a minimum:
  (a) have regard to significant shifts in the entity's fraud risk, threat and operating environment;
  (b) include an assessment of the appropriateness of the existing fraud control measures and mitigation controls; and
  (c) review and, where necessary, update the goals and strategic objectives in its fraud control plan, including:
    (i) record whether each goal and strategic objective has been met; and
    (ii) update the goals and strategic objectives for the next year.

(6) As soon as practicable after each review, an accredited entity must make all necessary amendments to its fraud control plan.

(7) All changes to the entity's fraud control plan must be approved in writing by the accredited entity's fraud controller.

Division 4—Incident detection, investigation, response and reporting

4.33 Incident monitoring and detection

(1) An accredited entity must implement and maintain appropriate mechanisms for:
  (a) preventing and detecting digital ID fraud incidents; and
  (b) alerting the entity's personnel to digital ID fraud incidents.

(2) Without limiting subsection (1), the mechanisms must include an accessible process for personnel, individuals, enforcement bodies and other relevant entities to report digital ID fraud incidents on a confidential basis.

4.34 Incident investigation, management and response

(1) An accredited entity must investigate digital ID fraud incidents unless the incident has been referred to, and has been accepted by, an enforcement body.

(2) An accredited entity must ensure that its personnel whose duties relate to conducting fraud investigations are appropriately qualified and trained to carry out those duties.

(3) An accredited entity must implement and maintain mechanisms for responding to digital ID fraud incidents, including, procedures to:
  (a) document the entity's processes for responding to digital ID fraud incidents and how it will investigate such incidents; and
  (b) include appropriate criteria for making timely decisions at each critical stage in response to a digital ID fraud incident.

(4) If an accredited entity cannot investigate a digital ID fraud incident because the entity does not hold personal information relevant to the incident, the entity must take reasonable steps to assist with the fraud investigation being conducted by other participants in the same digital ID system.

Example: Reasonable steps may include providing information relevant to the incident to another participant in the digital ID system where the entity is authorised to disclose such information.

4.35 Record keeping

An accredited entity must keep records of:
  (a) decisions to use civil, administrative or disciplinary procedures, or to take no further action, in response to a digital ID fraud incident; and

(b) the entity's investigation of and responses to digital ID fraud incidents.

Part 4.3—Privacy

4.36 Privacy governance code

In this Division:

privacy governance code means the *Privacy (Australian Government Agencies — Governance) APP Code 2017*.

agency has the same meaning as in the privacy governance code.

4.37 Compliance with privacy governance code

An accredited entity which is not an agency must comply with the privacy governance code in respect of its accredited services and DI data environment as if the entity were an agency for the purposes of the code.

Note: The privacy governance code includes requirements that agencies have a privacy officer, privacy champion, privacy management plan, register of privacy impact assessments, privacy education and training. Agencies must also conduct a privacy impact assessment for all high privacy risk projects and regularly review their internal privacy processes.

4.38 Privacy policy

(1) An accredited entity must have, maintain and comply with a privacy policy covering its accredited services and DI data environment.

(2) The entity's privacy policy must:
   (a) be written in a clear and simple manner, using plain language that is easy to understand;
   (b) provide sufficient detail about the collection, use and disclosure of personal information related to the entity's accredited services so as to enable an individual to understand how their personal information is collected, used and disclosed; and
   (c) be separate to the privacy policy for its other business and organisational functions.

(3) An entity which is accredited as more than one kind of accredited entity, must have and maintain either:
   (a) separate privacy policies and privacy management plans for each kind of accredited entity it is accredited as; or
   (b) distinct sections in its privacy policy and privacy management plan for each kind of accredited entity it is accredited as.

4.39 Review

An accredited entity must review its privacy policy and privacy management plan at least once in every reporting period.

4.40 Providing information about express consent

An accredited entity with public-facing accredited services and which is required to obtain the express consent of an individual must ensure that the process and description for an individual to provide express consent, or to withdraw or vary that consent, is in clear, simple and accessible terms.

4.41 Enduring consent

(1) If an individual gives an accredited entity consent for any future collection, use or disclosure of the individual's personal information (***enduring consent***), the enduring consent expires 12 months after the consent was given.

(2) An accredited entity with public-facing accredited services and which collects enduring consent from individuals must provide a clear and simple process for an individual to withdraw or vary that consent.

(3) An accredited entity must not rely on enduring consent given by an individual that has expired or been withdrawn.

4.42 Data minimisation principle

(1) An accredited entity must only collect personal information in connection with its accredited services that is reasonably necessary for the entity to provide its accredited services.

(2) An accredited entity must ensure that personal information disclosed to a relying party for the purposes of the relying party providing a service to an individual, or enabling the individual to access a service, is limited to the individual's personal information that is required for those purposes by:

(a) the accredited entity's information technology system having the functionality for the relying party to select the attributes of the individual that it requires to provide the service, or access to the service, to that individual; and

(b) providing only the selected attributes to the relying party.

4.43 Use of DVS and FVS for providing accredited services

An accredited identity service provider that obtains identification information using a DVS or FVS (within the meaning of those terms in the *Identity Verification Services Act 2023*) is authorised to use that information to create a data profile of the person for the

sole purpose of the accredited identity service provider providing its accredited services to the individual to whom the information relates.

Note: Section 53 of the Act prohibits data profiling to track online behaviour except in limited specified circumstances.

4.44 Disclosure of personal information for fraud activities

An accredited entity must notify individuals that the entity may use and disclose the individual's personal information to detect, manage and investigate digital ID fraud incidents.

4.45 Privacy awareness training

An accredited entity must ensure that each of its personnel whose duties relate to its accredited services or DI data environment completes privacy awareness training covering its privacy policy, privacy management plan and compliance with the additional privacy safeguards in Chapter 3 of the Act and this Part:

(a) before starting work on those duties; and

(b) at least once in every 12-month period thereafter.

4.46 Data breach response plan

(1) An accredited entity must have, maintain and comply with a data breach response plan that includes a description of the actions to be taken by the entity in the event of a data breach or suspected data breach involving its accredited services or DI data environment.

(2) The data breach response plan must:

(a) identify the roles and responsibilities of personnel involved in managing a data breach;

(b) include both a communication plan and guidance for personnel as to when and how information related to a data breach is to be:

(i) escalated within the entity;

(ii) notified to individuals affected by the data breach;

(iii) notified to a third party, including notifications required by law; and

(c) not be inconsistent with the entity's fraud control plan or system security plan.

(3) The data breach response plan for the accredited entity's accredited services and DI data environment must be separate from any data breach response plan in respect of its other business or organisational functions.

(4) An accredited entity must review and, if required, update its data breach response plan at least once in every reporting period.

4.47 Record keeping

An accredited entity must:

(a) keep records of its decisions to use civil, administrative or disciplinary procedures, or to take no further action, in response to a data breach; and

(b) keep records of the entity's investigation of and response to data breaches.

Part 4.4—Accredited services must be accessible and inclusive

4.48 Application

This Part applies for the purposes of subsection 30(1) of the Act (*Accredited services must be accessible and inclusive*).

4.49 Reporting on accessibility

Once in every reporting period, an accredited entity must prepare a report detailing for that reporting period:

(a) reasonable steps taken by the entity to ensure its accredited services are accessible for individuals who experience barriers when creating or using a digital ID; and

(b) reasonable steps the entity proposes to take in the next reporting period to continuously improve the accessibility of its services.

Note 1: See subsection 30(1AA) of the Act.

Note 2: The report must be included in the annual report provided to the Digital ID Regulator as part of the entity's annual review–see Chapter 6.

4.50 Accessibility requirements

(1) An accredited entity must:

(a) provide individuals with a clear and simple description of the entity's accredited services;

(b) present public-facing information related to its accredited services in a clear and simple manner, using plain language that is easy to understand; and

(c) take reasonable steps to ensure its public-facing information related to its accredited services is available in multiple accessible formats.

(2) For the purposes of paragraph 30(2)(a) of the Act, an accredited entity must comply with Level A conformance specified in WCAG Version 2.1 by ensuring its web pages (within the meaning of that term in the WCAG) satisfy the Level A Success Criteria specified in WCAG version 2.1.

(3) An accredited entity must take reasonable steps to comply with Level AA conformance as specified in WCAG version 2.1.

Note: At the time these rules were made, located at https://www.w3.org/TR/WCAG21/

(4) For the purposes of paragraph 30(2)(b) of the Act, an accredited entity with public-facing accredited services and public-facing

information related to its accredited services, when considering the accessibility of those services and information, must have regard to:

(a) item 3 (*Information and the operation of the user interface must be understandable*) of the WCAG;

(b) the 'Optional Component of a Conformance Claim' as specified in the WCAG; and

(c) the *World Wide Web Access: Disability Discrimination Act Advisory Notes* published by the Australian Human Rights Commission.

Note: At the times these rules were made, located at https://humanrights.gov.au/our-work/disability-rights/world-wide-web-access-disability-discrimination-act-advisory-notes-ver

Note 2: See also Division 2 (*Useability testing*) and Division 3 (*WCAG testing*) which set out requirements to test compliance with requirements related to accessible and inclusive accredited services.

(5) For the purposes of paragraph 30(2)(e)) of the Act—an accredited entity with public-facing accredited services must:

(a) provide assisted digital support to individuals who may experience barriers when creating or using a digital ID; and

(b) publish details of such support.

Example: Assisted digital support may include a monitored email address, a chat function, call centre or a telephone support line. Alternative channels may include an in-person shopfront.

(6) An accredited entity with public-facing accredited services must have written processes and procedures to:

(a) allow individuals to seek assistance or otherwise resolve disputes or complaints in relation to the entity's accredited services;

(b) obtain and record feedback from individuals about the useability and accessibility of the entity's public-facing accredited services; and

(c) where appropriate, incorporate such feedback into the design of its DI data environment.

4.51 Journey map

(1) An accredited entity with public-facing accredited services must create and maintain an end-to-end journey map of information flows which must be consistent with the map of information flows in the entity's most recent privacy impact assessment involving its accredited services and DI data environment.

(2) The journey map must:

(a) be in the form of one or more visualisations or diagrams;

(b) depict the stages and user interfaces an individual will go through when interacting with the entity's public-facing accredited services, including:

Rule 4.51

(i) each interface involving verification or authentication in relation to an individual; and

(ii) notices in relation to privacy, including notices or information required to be given to individuals in respect of privacy matters; and

(iii) any other information required by these rules to be given to individuals; and

(a) detail alternative channels (if any) available to the individual to complete a specific activity.

Part 4.5—Biometric information: testing and fraud activities

4.52 Requirements where biometric information is used for testing activities

(1) For the purposes of paragraph 49(6)(c) of the Act, an accredited entity that uses biometric information of an individual for the purpose of undertaking testing in relation to the information must comply with this rule.

Note: Section 51 of the Act specifies when biometric information must be destroyed.

Purposes for which testing may be conducted

(2) An accredited entity may undertake testing using biometric information for one or more of the following purposes and for no other purposes:

(a) to identify whether the thresholds of its technology for presentation attack detection are set correctly, including that, active 'spoofing' attacks on the technology will be correctly rejected;

(b) to identify issues associated with the performance and accuracy of its technology for presentation attack detection;

(c) to optimise its technology for presentation attack detection to improve its useability, performance and accuracy;

(d) to optimise controls that account for variances in image quality;

(e) to identify issues associated with the performance and accuracy of the biometric matching algorithm;

(f) to optimise the biometric matching algorithm to improve its performance and accuracy; or

(g) to measure any system demographic biases related to the quality of the biometric information.

Circumstances in which testing is conducted

(3) Testing using biometric information must be conducted only in the following circumstances:

(a) where the testing is unable to be conducted effectively by processing synthetic or anonymised data rather than biometric information of an individual;

(b) by a person with appropriate skills, experience and qualifications to conduct the testing; and

(c) in accordance with:

(i) the entity's system security plan;

(ii) a policy for working with human test subjects published by a national or international body; and

(iii) a testing plan that includes the information specified in subrule (5).

(4) The information for the test plan is:

(a) the objectives of the testing;

(b) the methodology to be used to conduct the testing, including:

(ii) the source and type of test data used; and

(iii) a description of the biometric information and the sample sizes to be used;

(c) the test frequency and duration of testing;

(d) how the biometric information will be stored and protected during the period of the testing; and

(e) how the biometric information will be destroyed at the end of the testing period.

Note: For paragraph (5)(d), ISO 24745 *Information security, cybersecurity and privacy protection—Biometric information protection* outlines how to protect biometric information that is stored.

(5) An accredited entity must ensure that its testing is conducted in accordance with the requirements of one or more policies covering the ethical use of biometric information, being policies and guidelines that ensure biometric systems do not selectively disadvantage or discriminate against any group.

Reporting of test results

(6) For each reporting period, the accredited entity must prepare a report detailing the results of any testing conducted in that reporting period and containing the following information:

(a) the total number of transactions involving biometric information;

(b) the number of transactions tested;

(c) the number of individuals whose biometric information was used for testing;

(d) whether the testing resulted in the entity taking action to respond to issues identified during the testing;

(e) an assessment as to whether the retention, use and disclosure of the biometric information for testing continues to be an effective mitigation measure against digital ID fraud risks, commensurate with the cyber security risk of retaining the biometric; and

(f) in respect of testing conducted for a purpose specified in paragraph (2)(c) or (d)—whether the testing effectively and ethically detected and corrected any bias identified in the biometric matching algorithm or presentation attack detection technology so as not to selectively disadvantage or

discriminate against any group whose biometric information used.

Example: For paragraph (e), the entity's assessment could include consideration as to whether tests using biometric information has improved the thresholds of the presentation attack detection system to effectively reject malicious actors.

4.53 Requirements where biometric information is used for fraud activities

For paragraph 49(8)(c) of the Act, an accredited entity that uses biometric information of an individual for the purposes of preventing or investigating a digital ID fraud incident must conduct the fraud-related activities in accordance with written ethical principles aimed at avoiding disadvantage to, or discrimination against, individuals.

Note: Section 51 of the Act specifies when biometric information must be destroyed.

Part 4.6—Review of DI data environment and statement of scope and applicability

4.54 DI data environment

At least once in every reporting period, an accredited entity must review the boundaries of its DI data environment:

(a) in accordance with rule 2.1 as if the references in that rule to 'applicant' were to the 'accredited entity'; and

(b) update the documented boundaries of its DI data environment to ensure it has correctly and completely defined and documented the boundaries of the DI data environment current at the time of the review.

4.55 Statement of scope and applicability

An accredited entity must review its statement of scope and applicability for completeness and accuracy:

(a) when it becomes aware of a material change to the extent and nature of threats to its DI data environment; or

(b) where no such material changes occur—at least once in each reporting period.

Chapter 5—Requirements when providing accredited services

Part 5.1—Preliminary

5.1 Definitions

In this Chapter:

ASP means an accredited attribute service provider.

alternative proofing process**—**see Subdivision C of Division 2 of Part 5.2.

ISP means an accredited identity service provider.

IXP means an accredited identity exchange provider.

Part 5.2—Accredited identity service providers

Division 1—Generating, managing, maintaining or verifying a digital ID

5.2 General requirements

(1) When generating a digital ID, an ISP must:

(a) other than where the ISP is generating a digital ID in accordance with an alternative proofing process:

(i) comply with the requirements in this Part applicable to the accredited service being provided and the manner of providing that service; and

(ii) comply with the Accreditation Data Standards applicable to the accredited service being provided and the manner of providing that service; and

(iii) verify the identity of the individual using only documents or other credentials of a kind listed in Schedules 1 to 4 which are verified in accordance with the requirement in column 2 of the relevant schedule; and

(b) at the time of generating the digital ID:

(i) bind an identity proofing level to the digital ID by complying with each requirement listed in column 1 of the IP Levels Table where that requirement is specified as 'must' or 'yes' in the column for the particular identity proofing level to be bound to the digital ID;

(ii) for a reuseable digital ID—bind one or more authenticators to the digital ID; and

(c) must not assert an identity proofing level or authentication level for a digital ID unless:

(i) other than where the ISP is generating a digital ID in accordance with an alternative proofing process—each of the requirements in the IP Levels Table for that identity proofing level has been met; and

(ii) each of the requirements in the AL Table for that authentication level has been met.

(2) An ISP must not assert that its processes for a particular identity proofing level creates assurance for that level that is similar or equivalent to a higher identity proofing level.

5.3 Digital IDs and children

(1) An ISP must not generate a digital ID for an individual if the individual requesting the generation of the digital ID is less than 15 years old.

(2) If the ISP is generating a digital ID for an individual at IP Level 1, the ISP will not breach subsection (1) if it requires the individual seeking to generate a digital ID to confirm that they are 15 years or over and the individual gives that confirmation in writing.

Note: For IP Level 1, the individual is not required to provide identity documentation to the ISP that would allow the ISP to independently verify the individual's age.

5.4 One-off digital IDs

An ISP accredited to generate a digital ID that is to be used once only (***one-off digital ID***) must not retain an attribute of an individual once the attribute has been disclosed to the relying party in a transaction, unless the ISP is required by law (including the Act and these rules) to retain that attribute and the attribute is retained in accordance with that law.

5.5 Expiry of a reusable digital ID

(1) A reuseable digital ID is taken to have expired in the following circumstances:

(a) for a digital ID with an identity proofing level of IP1 Plus or IP2—where a document or other credential listed in Schedule 1 to 4 of these rules relating to the individual has not been verified by an ISP within 5 years after the date that the digital ID was created, or 5 years after the credential was last verified; or

(b) for a digital ID proofed to IP2 Plus, IP3 and IP4—where biometric binding in respect of the individual's digital ID has not been conducted by an ISP for a period of 5 years after the date that the digital ID was created or 5 years after biometric binding was last completed.

(2) An ISP must not allow use of a digital ID that has expired.

5.6 Step-up of an identity proofing level

(1) An ISP may step-up an individual's identity proofing level for a reuseable digital ID if:

(a) requested by the individual;

(b) the ISP is accredited to conduct identity proofing at the higher identity proofing level; and

(c) before starting the step-up process, the individual authenticates to the required authentication level of the higher identity proofing level as required by item 14 in the IP Levels Table.

(2) When completed, the ISP must notify the individual of the new identity proofing level bound to their digital ID.

5.7 Updating and correcting attributes

(1) An ISP must allow an individual to update or correct an attribute that the ISP has bound to the individual's digital ID.

(2) Before binding the updated or corrected attribute to the digital ID of the individual, the ISP must:
(a) require the individual to authenticate to the authentication level already bound to the digital ID; and
(b) verify the attribute in accordance with the relevant requirements in the IP Levels Table.

(3) If the individual's names (family names, given names, middle names) or date of birth are not consistent across documents or other credentials presented for verification, the ISP must conduct further verification using a linking credential and must do so in accordance with the requirements in the IP Levels Table.

5.8 Suspension of a digital ID

If an individual requests the ISP to suspend the individual's digital ID, the ISP must:
(a) confirm the legitimacy of the request;
(b) as soon as practicable after confirming the legitimacy of the request, suspend the use of the digital ID for the period requested;
(c) following a suspension, notify the individual of the suspension and the process to reactivate their digital ID.

Note: See rule 5.10 for reactivation of a suspended digital ID.

5.9 Digital IDs affected by a fraud or cyber security incident

(1) Where the verification of, update to, or use of, a digital ID is identified as a suspected digital ID fraud incident or a suspected cyber security incident, an ISP must:
(a) verify that the digital ID has not been compromised;
(b) take reasonable steps to confirm that the individual has effective control of their digital ID; and
(c) if the ISP has not been able to confirm that the individual has effective control of their digital ID, suspend the use of the digital ID.

Suspected compromised digital ID

(2) If an ISP detects a digital ID fraud incident or cyber security incident in relation to an individual's digital ID and suspects that the digital ID has been, or is likely to be, compromised, the ISP must suspend that digital ID.

5.10 Reactivating a suspended digital ID

(1) When reactivating a digital ID suspended because of a cyber security incident or digital ID fraud incident, the ISP must ensure the individual completes identity proofing at the same identity proofing level of the suspended digital ID.

(2) When reactivating a digital ID suspended at the request of the individual, the ISP must ensure:

(a) the individual completes identity proofing at the same identity proofing level of the suspended digital ID and that the attributes presented by the individual can be linked to the attributes which comprise the suspended digital ID; or

(b) the individual completes biometric binding using a document or other credential whose attributes can be linked to the current attributes which comprise the suspended digital ID.

(3) The ISP is not required to reactivate a suspended or deactivated digital ID where the ISP no longer holds the relevant information that would enable it to do so.

Division 2—Identity proofing and use of credentials

Subdivision A—Identity proofing

5.11 IP Levels Table

(1) The IP Levels Table:

(a) specifies six identity proofing levels and the requirements to be met for each of those identity proofing levels when an ISP is binding an identity proofing level to a digital ID of an individual; and

(b) sets minimum requirements only for each identity proofing level, and does not restrict an ISP from applying, for a particular proofing level, the requirements for a higher proofing level (subject to the entity's accreditation conditions).

Example: An ISP may use biometric binding to verify the identity of the individual as part of their fraud controls for IP2, although that is not required for IP2. However, the ISP cannot do so unless authorised to collect the biometric information by an accreditation condition and cannot assert that its IP2 assurance is similar or equivalent to a higher IP level (see subrule 5.2(2)).

IP Levels Table

Item	Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
1	Username chosen by the individual is unique:	Must	Must	Must	Must	Must	Must
2	Checks undertaken by the ISP to establish that the identity is unique:	—	Must	Must	Must	Must	Must
3	A check undertaken by the ISP that the identity is not that of a deceased person:	—	Recommended	Recommended	Recommended	Must	Must
4	Verification of the link between the individual and the claimed identity to occur through biometric binding:	—	—	—	Must	Must	Must
5	All original, physical documents or other credentials to be provided and the individual witnessed in-person:	—	—	—	—	—	Must
6	Checks to be undertaken against information or records held within the ISP to confirm the identity is not known to be used fraudulently:	—	Must	Must	Must	Must	Must

Rule 5.11

Item	Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
7	Personnel undertaking identity proofing processes, including visual verification, are required to be provided with tools and training to detect fraudulent attributes, and document or other credentials, before starting work on these duties and annually thereafter:	—	Must	Must	Must	Must	Must
8	Translation by a National Accreditation Authority for Translators and Interpreters accredited translator of documents or other credentials in languages other than English required:	—	—	Recommended	Recommended	Must	Must
9	The individual's given name, middle name (if any), surname and date of birth, as they appear on a document or other credential being used for verification, must be	No	Yes	Yes	Yes	Yes	Yes

Item	Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
	verified using only source verification or technical verification:						
	Credentials required for verification						
10	Verification of a CoI credential must be undertaken:			Yes, unless a photo ID used (see item 11).	Yes, unless a photo ID used (see item 11).	Yes	Yes
11	Verification of a photo ID must be undertaken:	—	Yes, unless a UitC credential is used (see item 12).	Yes, unless a CoI credential is used (see item 10).	Yes, unless CoI credential used (see item 10).	Yes	Yes
12	Verification of a UitC credential must be undertaken:	—	Yes, unless a photo ID is used (see item 11)	Yes	Yes	Yes	Yes, but 2 UitC credentials must be used for verification
13	Verification of a linking credential must be undertaken if attributes vary across documents or other credentials:	—	—	Yes	Yes	Yes	Yes
14	Authenticator levels to be bound to a digital ID:	AL1, AL2 or AL3	AL2 or AL3	AL2 or AL3	AL2 or AL3	AL2 or AL3	AL3

Note 1: For item 2, the checks undertaken by the ISP may be done through checking the ISP's records for a digital ID with the same attributes.

Note 2: For item 6, the checks undertaken by the ISP may include checks against the ISP's registers of known fraudulent identities.

Note 3: For item 14, see the Accreditation Data Standards for the requirements to be met before an authentication level for a digital ID can be asserted.

5.12 Verification using an Australian passport

(1) For items 10 (*verification of a CoI credential*) and 11 (*verification of a photo ID*) in the IP Levels Table, if an Australian passport is being used for identity proofing for IP Level 3, that credential can be used simultaneously to satisfy the requirements both for a CoI credential and a photo ID.

(2) For item 10 in Table 1 (*verification of a CoI credential*), if an Australian passport is being used for identity proofing for IP Level 4, that credential can be used to satisfy either the requirements for a CoI credential or a photo ID, but not both.

5.13 Technical verification of credentials

Where an ISP is using technical verification to verify an Australian passport or a foreign ePassport, the ISP must:

(a) comply with the sections of the ICAO Doc 9303 Standard that apply when using remote public key infrastructure to verify an ePassport; and

(b) for an Australian passport, review the certificate revocation list, published by the Department of Foreign Affairs and Trade, to establish whether the passport has been cancelled; and

(c) for a foreign passport, where the issuing country publishes a certificate revocation list, review that list to establish whether the passport has been cancelled.

Note: At the time these rules were made, the certificate revocation list for Australia passports was located at https://www.passports.gov.au/australian-country-signing-certificate-authority-csca

5.14 Source verification using non-government credentials

Where an ISP is using a document or other credential issued by an entity other than an entity covered by subsection 50(3) of the Act, the ISP must:

(a) use approved cryptography to establish a trusted and secure connection with the authoritative source for that credential; and;

(b) ensure the document, other credential or attributes, being verified are current.

Note: Entities covered by subsection 50(3) of the Act are government entities.

5.15 Visual verification

An ISP must:

(a) for visual verification of a document or other credential—ensure visual verification is conducted only by personnel who have been appropriately trained to conduct such verification; and

(2) not use visual verification if source verification or technical verification has been conducted and the result indicates that the document or other credential is not legitimate.

Subdivision B—Verification using biometric information

5.16 Application

This Subdivision:

(a) applies to an ISP conducting identity proofing at levels IP2 Plus, IP3 or IP4; and

(b) sets out the requirements for biometric binding when conducting identity proofing at those levels.

5.17 Requirements for biometric binding

(1) Biometric binding must be conducted by using either:

(a) online biometric binding; or

(b) local biometric binding.

(2) Source verification of a photo ID that will be used for biometric binding must be completed before starting the biometric binding process.

(3) Where the photo ID used is a foreign passport, including a foreign ePassport, the following requirements apply:

(a) the passport must be linked to a visa that has been source verified; and

(b) the biometric binding process must not be conducted until the linking of the visa and passport is verified.

5.18 Requirements for online biometric binding

(1) Online biometric binding must capture an acquired image and conduct at least one of the following on the image:

(a) technical biometric matching;

(b) source biometric matching; or

(c) eIDVT biometric matching.

(2) An acquired image must not be used for biometric binding unless:

(a) an image quality profile of the acquired image has been created; and

(b) a quality threshold for the acquired image has been applied and the threshold takes into account possible fraud risks and cyber security risks.

(3) Online biometric binding must take into account the characteristics of biometric image quality described by ISO 29794-5 when generating the image quality profile of the acquired image.

Note: At the time these rules were made, details for ISO 29794-5-1 are located at [***add***].

(4) An ISP must record evidence of the characteristics used in generating the image quality profile and quality threshold for the acquired image (both as required by paragraph 2).

Example: Evidence of the characteristics may include image format, image resolution, contrast exposure or noise, colour depth and background characteristics.

Note: Details may be recorded in technical documents or third-party service level agreements, and may include demonstrations of the biometric capability of the accredited service in action and internal quality assurance processes for acquired image capture, including how a system determines meeting an image quality score threshold.

(5) An ISP must implement automated quality controls in its biometric capability and have appropriate user-interface instructions that direct an individual to capture an image using the biometric capability that meets the image quality profile for the acquired image.

(6) An ISP must comply with the following requirements when conducting online biometric binding:

(a) online biometric binding must be completed in a single continuous workflow;

(b) liveness detection must be included as part of presentation attack detection;

(c) presentation attack detection must be used at the point of capture of the acquired image;

(d) the capture of the acquired image and presentation attack detection must be completed, as part of the same process, before the acquired image is submitted for biometric binding; and

(e) presentation attack detection technology that incorporates data captured by both the data capture subsystem and through system level monitoring, as described by ISO 30107-1, must be used.

Note: At the time these rules were made, details for ISO 30107-1 are located at [***add***].

5.19 Requirements for local biometric binding

(1) Local biometric binding must be conducted by an assessing officer in the physical presence of the individual and must use one or more o f the following processes:
  (a) technical biometric matching;
  (b) source biometric matching;
  (c) eIDVT biometric matching.

(2) However, if those processes are unavailable to the accredited entity for a kind of photo ID, manual face comparison may be conducted.

(3) While conducting local biometric binding, access to biometric information and the biometric capability of the ISP must be restricted to the assessing officers conducting the binding.

(4) If an acquired image is being captured as part of local biometric binding, an image quality profile must be developed and applied in accordance with rule 5.20 (*requirements for online biometric binding*).

(5) Local biometric binding must be conducted only at a location that is named in the ISP's fraud control plan and system security plan as able to be used for that purpose.

5.20 Requirements for technical biometric matching

(1) Technical biometric matching of an acquired image must only be conducted using an Australian passport or foreign ePassport where that passport has first been technically verified in accordance with rule 5.13.

(2) A biometric matching algorithm must only be used to conduct one-to-one biometric matching between the acquired image and the image on the document or other credential.

5.21 eIDVT biometric matching

(1) eIDVT biometric matching must be conducted using only one of the following photo IDs presented by the individual to a biometric sensor (***physically presented***) at the time the matching is being conducted:
  (a) driver's licence issued under a law of a State or Territory;
  (b) proof-of-age card issued by or on behalf of a State or Territory; or
  (c) Australian passport.

Note: A biometric sensor includes a camera within a phone or a webcam.

(2) The ISP must ensure that its eIDVT includes processes to:
  (a) identify and verify that the photo ID physically presented is authentic and original;
  (b) detect the presence of false, counterfeit, forged or inconsistent photo IDs; and
  (c) determine whether the relevant photo ID was physically present at the time of capture, including by:
    (i) implementing testing for document liveness;
    (ii) not allowing individuals to submit previously captured images of photo IDs; and
    (iii) making checks to ensure the image acquired of the photo ID is of the original document or other credential, and not a second-generation image such as an image of an image of a document or other credential or a photocopy of a document or other credential.

(3) An entity's eIDVT must:
  (a) use optical character recognition (OCR) to convert an image of an acquired document or other credential into a machine-readable text format as part of the automated document verification process;
  (b) ensure the OCR technology is effective and performs checks for information inconsistency, data quality and accurate information extraction; and
  (c) not use any manual human review processes.

  Example: The checks referred to in paragraph (b) may include image pre-processing, text recognition, data extraction and conversion into a digitised format (such as JSON, XML or delimited text), checksum values to reduce the likelihood of character substitution errors, and self-learning models for continuous improvement

(4) An ISP must only process a photo ID through eIDVT that is:
  (a) successfully verified as authentic; and
  (b) determined by the entity as having been physically present at the time of capture by testing for document liveness.

(5) When processing a photo ID through eIDVT, the entity must ensure that the eIDVT:
  (a) identifies at least five security features in the photo ID and compares the security features against an identity document template;
  (b) compares the photo ID's expiry date to the date on which the matching is attempted;
  (c) ensures the facial image on the photo ID is genuine and has not been altered, changed or modified in any way;
  (d) only processes images with a resolution of at least 300 dpi; and
  (e) limits the number of attempts to verify the authenticity of a photo ID using eIDVT to five.

(6) In this rule, ***identity document template*** means a model representation of a particular identity document that is used to verify an acquired image of an identity document of that type.

Example: An identity document template may include text locations, colours and other graphical elements, security features, and locations of facial biometrics for identity documents that are also photo IDs.

(6) The ISP must destroy images of processed photo IDs immediately after completion of the eIDVT biometric matching, except for images of photo IDs classified by the eIDVT as not genuine, which may be retained by the entity for fraud activities in accordance with subsection 49(8) of the Act.

(7) The ISP must not use a facial image acquired from a photo ID for eIDVT biometric matching unless:

(a) the entity has created an image quality profile for the facial image;

(b) the entity has applied a quality threshold to the facial image; and

(c) the image has passed the quality threshold for the facial image quality profile.

(d) the ISP must follow the requirements described by ISO 29794-5 when determining the method to be used for generating the image quality profile of the facial image acquired from the photo ID.

Note: At the time these rules were made, details for ISO 29794-5 are located at [***add***].

(8) The ISP must use a biometric matching algorithm to conduct one-to-one verification matching between the acquired image of the individual and the facial image acquired from the photo ID.

(9) The ISP must ensure that the verification, identification and detection processes do not result in any damage to the photo ID being processed.

5.22 Requirements for manual face comparison

(1) Manual face comparison must be conducted using only an original, physical, photo ID presented in person by the individual at the time the manual face comparison is conducted.

(2) An ISP must:

(a) not permit an assessing officer to conduct manual face comparison unless the assessing officer has received awareness training in accordance with the guidance provided by the *Guide for Facial Comparison Awareness Training of Assessors* published by the Facial Identification Scientific Working Group:

(i) before starting to conduct manual face comparisons for the ISP; and

(ii) at least once in every 12 months thereafter;

Note: At the time these rules were made, the *Guide for Facial Comparison Awareness Training of Assessors* was located at [***add***].

(b) provide assessing officers with a current reference document outlining practical steps and guidance when conducting manual face comparison;

(c) implement and maintain procedures to detect any fraudulent activities conducted by assessing officers when conducting manual face comparison; and

Note: Details of the procedures must be included in the accredited entity's fraud control plan.

(d) record in its cyber security plan and fraud control plan its procedures to implement and maintain quality control and quality assurance procedures for manual face comparison decisions made by assessing officers and ensure assessing officers comply with those procedures.

Subdivision C—Alternative proofing processes

5.23 Accessible and inclusive services

This Subdivision:

(a) applies for the purposes of subsection 30(1) of the Act (*Accredited services must be accessible and inclusive*); and

(b) sets out a process for identity proofing for an individual who does not possess, and is unable to obtain, the documents or other credentials necessary to create a digital ID at the identity proofing level sought by the individual.

5.24 Exceptional use case

Exceptional use case means a case where an individual:

(a) does not possess the documents or other credentials required to be provided to create a digital ID at the identity proofing level sought by the individual; and

(b) is unable to obtain the document or other credentials in a reasonable timeframe, having regard to the circumstances as to why the individual is unable to obtain the documents or other credentials.

5.25 Requirements for an alternative proofing process

(1) An ISP may conduct an alternative proofing process only if it is authorised to do so by an accreditation condition and only in the circumstances specified in the conditions.

(3) An alternative proofing process may include one or more of the following:
   (a) acceptance of alternative kinds of document or other credentials;
   (b) verification of an individual's claimed identity with another individual who is a trusted referee, being a person who holds a position of trust in the community and whose identity has been verified to an equal or higher identity proofing level than the level requested for the alternative proofing process;
   (c) verification of an individual's claimed identity with a reputable organisation known to the individual for example, Aboriginal and Torres Strait Islander organisations may be able to verify the identity of an individual if no government record for that individual exists;
   (d) reliance on the identity proofing processes of a reputable organisation that has verified the identity of the individual to the requested identity proofing level;
   (e) an interview with the individual that satisfies the ISP of the consistency and legitimacy of the individual's claims, including the validity of the claimed identity;
   (f) where an individual lives in a remote area—provide an alternative to an in-person interview;
   (g) providing support to an individual to obtain a necessary document or other credential which may include assisting the individual to register their birth; or
   (h) another process for identity proofing for an individual as detailed in the entity's accreditation conditions.

(4) Before undertaking an alternative proofing process to create a digital ID for an individual, an ISP must:
   (a) be satisfied that an exceptional use case exists in respect of the individual;
   (b) conduct a risk assessment, including of the risks to relying parties that may rely on the individual's digital ID if created; and
   (c) prepare and maintain a report of the risk assessment that includes detail of the controls and risk-mitigation strategies to be implemented in response to the identified risks.

Division 3—Generating, binding, managing or distributing authenticators

5.26 General requirements

(1) When binding an authentication level to a digital ID, an ISP must ensure that the authentication level meets each requirement specified in column 1 of the AL Table for the particular authentication level in column 1, 2 or 3 of the AL Table.

(2) An ISP must not assert an authentication level for a digital ID unless each of the requirements in the AL Table for that authentication level has been met.

(3) Before authenticating the digital ID of an individual, an ISP must ensure that the authenticator presented by the individual has not expired or been suspended or revoked.

(4) Where the authentication level bound to an individual's digital ID is to be stepped-up to a higher authentication level, the individual must first authenticate to their digital ID using the existing authenticator bound to the digital ID.

(5) If an individual requests the ISP to suspend or revoke the individual's authenticator, the ISP must:
  (a) confirm the legitimacy of the request; and
  (b) as soon as practicable after confirming the legitimacy of the request, suspend or revoke the authenticator.

(6) An additional authenticator must not be bound to a digital ID unless the individual has first authenticated at least to the authentication level at which the new authenticator will be used.

(7) If an ISP issues authenticators that expire, an updated authenticator must be bound to a digital ID in a reasonable amount of time before the authenticator expires.

(8) When the individual authenticates to their digital ID using the new authenticator, the authenticator being replaced must be immediately revoked.

(9) If an ISP reasonably suspects that use of a kind of authenticator is, or would, result in an unacceptable risk to an individual, the ISP must as soon as practicable:
  (a) prevent further use of that authenticator;
  (b) notify individuals using that kind of authenticator of the security risk;
  (c) offer affected individuals at least one alternative authenticator at the authenticator level required to be bound to the individual's digital ID; and

(d) address any additional risks to individuals in the ISP's system security plan.

5.27 Physical authenticators

(1) A physical authenticator means one of the following:
   (a) look-up secrets;
   (b) single-factor one-time password device;
   (c) multi-factor one-time password device;
   (d) single-factor cryptographic software;
   (e) single-factor cryptographic device;
   (f) multi-factor cryptographic software;
   (g) multi-factor cryptographic device;
   (h) out-of-band devices.

(2) An ISP that conducts authentication using a physical authenticator, must:
   (a) provide individuals with clear instructions about how to protect the physical authenticator against theft or loss; and
   (b) have a mechanism in place to immediately suspend or revoke use of the authenticator if an individual notifies the ISP of the actual, or a suspected, loss or theft of their physical authenticator.

5.28 Authenticator that has been compromised

(1) If an ISP becomes aware that an individual's authenticator has been lost, stolen, damaged or duplicated without authorisation (***compromised authenticator***), the ISP must immediately:
   (a) suspend use of the authenticator;
   (b) revoke the authenticator; or
   (c) destroy the authenticator.

(2) Where an ISP reasonably suspects that a transaction involves a digital ID fraud incident or cyber security incident, the ISP must verify that the relevant authenticator has not been compromised.

(3) To facilitate secure reporting of a compromised authenticator by the individual to the ISP, the individual may authenticate to their digital ID using an alternative authenticator, but, if so, the alternative must be only a memorised secret or physical authenticator.

5.29 Step-up of an authentication level

An ISP may allow an individual to step-up the authentication level bound to their digital ID, but only where the individual has first authenticated to their digital ID using the existing authenticator bound to the digital ID.

5.30 Expired and renewed authenticators

(1) An ISP must not allow an individual to use an authenticator that has expired.

(2) As soon as practical after an authenticator has expired, or the ISP has confirmed that an individual has bound a renewed physical authenticator to their Digital ID, the ISP must ensure the individual has surrendered, or proved destruction of, a physical authenticator containing attribute certificates signed by the ISP.

5.31 Revocation and termination of an authenticator

(1) An ISP must promptly revoke an authenticator when:
   (a) an individual's digital ID associated with that authenticator ceases to exist;
   (b) requested by the individual; or
   (c) the ISP determines that the individual no longer meets its eligibility requirements.

Note: For (c), this may be because the individual has died or that the digital ID is fraudulent.

(2) As soon as practical after revocation of an attribute certificate or termination of the individual's authenticator, the ISP must require the individual to surrender, or prove destruction of, a physical authenticator containing attribute certificates signed by the ISP.

Division 4—Accessibility and useability

5.32 Application

This Division applies for the purposes of section 30 of the Act (*Accredited services must be accessible and inclusive*).

5.33 Verification services

(1) An ISP must provide support to individuals who need assistance during the identity proofing process, including providing clear instructions about how the individual can update their personal information held by the ISP.

(2) An ISP must provide individuals with a clear and simple description of each step of the identity proofing process, including a description of what the individual needs to do to complete each step and the technical requirements that must be met to complete identity proofing.

(3) An ISP must provide individuals with information about the technical requirements for using the ISP's technology information system.

Note: Technical requirements may include access to a mobile phone or webcam.

(4) An ISP must:

(a) provide individuals with information on the document or other credentials that may be requested to verify the individual's identity at a particular identity proofing level, including information on the combinations of documents or other credentials that will satisfy the request where more than one document or other credential is required;

(b) notify individuals whether a requested document or other credential is mandatory; and

(c) notify individuals of the consequences to the individual if they do not provide particular documents or other credentials.

(5) If a digital code is to be issued by the ISP to an individual as part of the identity proofing process, the ISP must first inform the individual in clear and simple terms of:

(a) the fact that the individual will receive a digital code from the ISP;

(b) the method by which the digital code will be issued; and

(c) what the individual is required to do with the digital code.

(6) An ISP must promptly notify the individual of the outcome of the identity proofing process as follows:

(a) if the identity proofing process has been successfully completed—provide the individual with confirmation regarding the successful identity proofing and information on next steps to be taken by the individual (if any);

(b) if the identity proofing process has been partially completed—provide the individual with confirmation of the:

(i) information, documents and other credentials (***information***) that will be destroyed by the entity;

(ii) information that will be retained by the entity and the period for which they will be retained; and

(iii) additional information to be provided by the individual in order to successfully complete the identity proofing process;

(c) if the identity proofing process has been unsuccessful—provide the individual with:

(i) where applicable, details of the ISP's alternative channels or support to complete the proofing process;

(ii) clear and simple instructions about how to use such alternative channels and support; and

(iii) an option to either:

(A) continue the proofing process using one or more such alternative channels; or

(B) not continue with the proofing process.

(7) If the individual elects to:

(a) continue with the proofing process, the ISP must ensure, to the extent practicable to do so, that the individual is not required to provide the same information already been provided to the ISP during the initial proofing process; or

(b) not continue with the proofing process, the ISP must:

(i) ensure that information provided by the individual during the proofing process is destroyed as soon as practicable after the individual's decision, unless it is necessary to retain the information to investigate a digital ID fraud incident; and

(ii) notify the individual of the information to be destroyed.

5.34 Authentication services

An ISP providing services involving authentication of an individual must provide individuals with information about the use and maintenance of their authenticator, including:

(a) instructions on how to use the authenticator;

(b) when the authenticator will expire; and

(c) what do to if the authenticator is forgotten, lost or stolen.

Part 5.3—Accredited attribute service providers

5.35 Verifying and managing a special attribute

(1) An ASP must only verify or manage an attribute of an individual if the particular kind of attribute is specified in the ASP's accreditation conditions as the attribute the ASP is accredited to verify and manage (***special attribute***).

(2) An ASP must:
  (a) determine the identity proofing level it requires for the purpose of providing its accredited services in respect of a special attribute of an individual; and
  (b) not provide an accredited service in respect of an individual unless the digital ID of the individual meets that identity proofing level.

5.36 Requirements when verifying a special attribute

When verifying a special attribute of an individual:
  (a) an ASP must ensure the special attribute is:
    (i) unique to the individual; and
    (ii) current at that time; and
  (b) must verify the special attribute with the authoritative source for that special attribute and must do so by:
    (i) establishing a trusted and secure connection with the authoritative source using approved cryptography, including where the ASP and the authoritative source are the same entity; and
    (ii) complying with requirements set by the authoritative source as to the information that must be provided to allow the authoritative source to confirm that the special attribute is unique to that individual.

5.37 Special attributes that are self-asserted

If a special attribute of an individual is self-asserted by the individual and not verified by the ASP, the ASP must inform an accredited entity or relying party seeking verification or disclosure of the special attribute of each of those facts.

5.38 Special attributes affected by a fraud or cyber security incident

(1) An ASP must not disclose a special attribute if the ASP is aware that the special attribute has been involved in a cyber security incident or digital ID fraud incident.

(2) If an ASP becomes aware that a special attribute has been involved in a cyber security incident or digital ID fraud incident, it must

immediately notify the authoritative source (if the ASP and the authoritative source are not the same entity).

Part 5.4—Accredited identity exchange providers

5.39 General requirements

An IXP must securely identify and authenticate each digital ID service provider and relying party involved in a transaction before conveying, managing or facilitating the flow of information between each participant.

5.40 Single sign on

(1) If an IXP provides single sign on, the IXP must:
  (a) allow a relying party to request that an individual authenticates to their digital ID regardless of whether a pre-existing authenticated session exists; and
  (b) implement a single logout mechanism.

(2) For a single sign on, if an IXP securely caches attributes obtained from an ISP or ASP for the duration of an authenticated session, the attributes of the individual must not be accessible to the IXP's personnel.

5.41 Digital ID system rules

(1) This rule applies to an IXP operating in a digital ID system:
  (a) other than the Australian Government Digital ID System; and
  (b) where one of more digital ID service providers participating in the digital ID system provides services in the system that are not accredited services.

(2) The IXP must ensure that the digital ID system in which the IXP operates is subject to system rules which:
  (a) are binding on an identity service provider (***unaccredited ISP***) that provides services in the digital ID system that are not accredited services;
  (b) are enforceable to the extent that the IXP, or another person able to enforce the system rules, can revoke the unaccredited ISP's participation in the digital ID system for non-compliance with the system rules; and
  (c) are not inconsistent with the Act and these rules.
  (d) require that all information conveyed or managed within the digital ID system is dealt with in accordance with approved cryptography as if rule 4.21 applied to the unaccredited ISP;
  (e) require that an unaccredited ISP must not disclose an attribute of an individual referred to in section 45 of the Act without the express consent of the individual; and

(f) conduct one-to-many matching of biometric information of an individual collected for the purposes of the identity service provider doing either or both of the following:
  (i) verifying the identity of the individual;
  (ii) authenticating the individual to their digital ID.

Chapter 6—Annual reviews

Part 6.1—Accredited entities to conduct annual reviews

6.1 General requirements

(1) Before the end of each reporting period for an accredited entity, the accredited entity must conduct an annual review in accordance with this Part.

(2) The accredited entity must, in respect of each reporting period:
  (a) prepare a report in accordance with Part 6.2; and
  (b) give a copy of the report to the Digital ID Regulator within 30 days of the end of the reporting period.

(3) Assurance assessments, systems testing and any other testing conducted for an annual review must be conducted as close as practical to the end of the reporting period for that review.

6.2 Reporting periods for transitioned accredited entities

(1) The reporting period for an accredited entity listed in column 2 of the following table is:
  (i) for the entity's first reporting period after the day the Act commences—the period beginning on the day the Act commences and ending on the date listed in column 3 of the table (***end date***); and
  (ii) for subsequent reporting periods—each 12-month period after the end date.

Column 1	**Column 2**	**Column 3**
Item	**Entity**	**Date by which the entity must complete its first annual assessment**
1	Services Australia	***[Table to be completed for transitioned accredited entities]***
2	Australian Taxation Office	

Note 1: The entities listed in the table are entities that are taken to be accredited on the day the Act commences – see the *Digital ID (Transitional and Consequential Provisions) Act 2024*.

Example: An entity which must complete its first annual review by 20 June 2025 must complete subsequent annual reviews by 20 June of each year.

6.3 Reporting periods for other accredited entities

The reporting period for an accredited entity not covered by rule 6.2 is:

(a) for the entity's first reporting period—the 12-month period starting on the day the entity's accreditation comes into force and ending 12 months after that date (***end date***); and

(b) for subsequent reporting periods—each 12-month period after the end date.

6.4 Scope of annual review

(1) ***Material change*** has the meaning given in subrule (4).

Review of changes

(2) An accredited entity must, for each reporting period:

(a) identify changes to the entity's accredited services and DI data environment that might affect the entity's ability to comply with its obligations under the Act, these rules or the Accreditation Data Standards;

(b) update the entity's statement of scope and applicability to address all such changes; and

(c) provide the updated statement of scope and applicability to each assessor conducting an assurance assessment or system testing for the entity.

(3) For each change identified, the accredited entity must:

(a) consider the impact of the change on the entity's accredited services and DI data environment;

(b) consider whether any change, and all changes considered cumulatively, might affect its ability to comply with the requirements of the Act, these rules or the Accreditation Data Standards;

(c) assess whether any change, and all changes considered cumulatively, results, or is reasonably likely to result, in:

(i) a material or adverse impact on the entity's accredited services or DI data environment; or

(ii) an adverse impact on the entity's ability to comply with the Act, these rules or the Accreditation Data Standards.

(4) Changes, alone or cumulatively, assessed as having, or likely to have, an effect referred to in paragraph (3)(c) are a ***material change***.

Response to material changes

(5) For each material change, the accredited entity must conduct:

(a) an assurance assessment or systems testing but only to the extent required to assess the effect of the material change and

to ensure, and demonstrate, that the entity continues to comply with the controls and requirements affected by the material change;

Note 1: A full assurance assessment or system testing is not required where the material change does not affect all controls. The assessment or testing can be limited to those controls that may be affected.

Note 2: 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—see rule 4.37 which applies the *Privacy (Australian Government Agencies- Governance) APP Code 2017* to accredited entities that are not agencies under the Privacy Act. That Code requires a privacy impact assessment for high privacy risk projects.

(b) technical testing to ensure the entity's information technology system continues to have the functionality necessary to meet the requirements specified in rule 2.5(1) but only to the extent that the material change relates to one of those requirements, and record in respect of that testing each of the matters specified in paragraph 2.55(2); and

(c) for an accredited identity service provider that conducts biometric binding or biometric authentication, testing for the presentation attack detection technology, the biometric matching algorithm, or the eIDVT in respect to the activities affected by the material change.

(6) For each reporting period, the accredited entity must review any condition imposed by the Digital ID Regulator relating to the collection and disclosure of restricted attributes by the entity to determine if the condition continues to be required.

6.5 Assurance assessments

Fraud assessment

(1) An accredited entity is required to conduct a fraud assessment in the reporting period after its first reporting period and thereafter in every alternate reporting period.

(2) Despite subrule 3.6(2), the fraud assessment may be conducted by an assessor who does not meet the additional requirements in that rule if:

(a) in the previous two years, a fraud assessment has been conducted by assessor who meets the requirements in subrule 3.6(2); and

(b) that assessor has stated in their previous report of the assessment that the entity's fraud management capability is sufficiently mature, including that the entity's personnel are sufficiently experienced in managing that capability, such that the entity's personnel can complete the next fraud assurance assessment.

Protective security assessment

(3) An accredited entity is required to conduct a protective security assessment in the reporting period after its first reporting period and thereafter in every alternate reporting period.

6.6 Penetration and presentation attack detection testing

Penetration testing

(1) For each reporting period, an accredited entity is required to conduct penetration testing and provide the entity's response to the assessor's report.

Note: For penetration testing, see rule 3.8; for the entity's response, see rule 3.18.

Testing for presentation attack detection

(2) An accredited identity service provider that conducts biometric binding or biometric authentication is required to conduct testing for presentation attack detection in the reporting period after its first reporting period and thereafter in every alternate reporting period.

Part 6.2—Accredited entities to provide annual reports

6.7 Content of annual report

The entity's report for each reporting period (***annual report***) must contain the information and documents required by this Part.

6.8 Where previous timeframes to address risks and recommendations not met

(1) This rule applies where an accredited entity's response to an assessor's report or a privacy impact assessment (***PIA***), whether the report or PIA was conducted in the reporting period under review or earlier:

(a) provides a timeframe for the entity to implement treatment to address an identified risk or a recommendation in the report or PIA; and

(b) the timeframe will not be met by the time the entity provides its annual report for the reporting period under review.

(2) The accredited entity must provide in its annual report details of when the treatment will be implemented and risks arising, or likely to arise, from the treatment not having already been implemented.

6.9 Information and documents

The entity's annual report must include the following information and documents:

(a) if the entity has updated the boundaries of its DI data environment, a copy of the updated documentation (see rule 4.54);

(b) if the entity has updated its statement of scope and applicability, a copy of the updated statement (see rule 4.55);

(c) if the accredited entity has conducted an assurance assessment or systems testing, a copy of the assessor's report and the entity's response;

(d) if the accredited entity has conducted testing for presentation attack detection, a copy of the presentation attack detection report;

(e) a copy of the accredited entity's cyber security risk assessment (see rule 4.7);

(f) a copy of the accredited entity's fraud risk assessment (see rule 4.25);

(g) a copy of the accredited entity's report on accessible services (see rule 4.49);

(h) in respect of accredited services provided by the accredited entity in a digital ID system other than the Australian Government Digital ID System—the following details for the reporting period:
  (i) the number (including nil) of digital ID fraud incidents and cyber security incidents, excluding attempted incidents, that occurred in the reporting period in relation to the entity's accredited services and DI data environment; and
  (ii) for each of those incidents:
    (A) the date of the incident;
    (B) a description of each type of incident and its severity; and
    (C) a description of the measures taken by the entity in response to the incidents covered by the report; and
(i) a copy of any privacy impact assessment involving the accredited entity's accredited services or DI data environment and a copy of the entity's response to an assessment;
(j) for an accredited identity service provider required to undertake biometric testing—the results of the biometric testing (see the Accreditation Data Standards for biometric testing);
(k) for an accredited identity service provider that conducts biometric binding or biometric authentication in accordance with the applicable type of biometric testing:
  (i) the results of the entity's testing of its biometric matching algorithm;
  (ii) the results of the entity's testing of eIDVT (if any); and
  (iii) evidence that the entity has completed testing of source biometric matching; and
(l) for an accredited identity service provider that conducted testing using biometric information of an individual for testing activities in the reporting period, a copy of the report of that testing (see subrule 4.52(6)).

6.10 Attestation statement

The report must include an attestation statement, signed by the accredited entity's accountable executive, that attests that in the reporting period to which the report relates:

(a) the entity has reviewed changes in accordance with rule 6.4 and correctly identified any material change;
(b) the entity has reviewed its:
  (i) system security plan;
  (ii) fraud control plan;
  (iii) disaster recovery and business continuity plan;

(iv) privacy policy;
(v) privacy management plan;
(vi) data breach response plan; and

(c) each of those plans is appropriate and adapted to respond to risks and threats, including emerging risks and threats, to the entity's accredited services and DI data environment;

(d) where a cloud service provider conducts penetration testing as referred to in paragraph 3.8(4)(b)—the entity is satisfied that that penetration testing covers the kinds of penetration testing in subrule 3.8(2);

(d) the entity is satisfied that a condition imposed by the DI Data Regulator relating to restricted attributes continues to be necessary and appropriate and, if not, a variation to the condition will be sought;

(e) the entity has complied with the Act, these rules and the Accreditation Data Standards, other than in respect of any non-compliance previously notified to the Digital ID Regulator in the reporting period; and

(f) the entity is not aware of any circumstances that might prevent or adversely affect the entity's ability to comply with the Act, these rules or the Accreditation Data Standards.

Chapter 7—Other matters relating to accreditation

Part 7.1—Matters related to attributes

7.1 Individuals must expressly consent to disclosure of certain attributes of individuals to relying parties

For the purposes of paragraph 45(f) of the Act, the following kinds of attributes are prescribed:

(a) to the extent not covered by section 45 of the Act, attributes of an individual that are on a document or other credential listed in Schedules 1 to 4;

(b) attributes that are derived from an attribute listed in paragraphs 45(a) to (e) of the Act or paragraph (a);

(c) a special attribute of an individual;

(d) an attribute that is self-asserted by the individual and not verified.

Example: For paragraph (b), information as to whether an individual is aged 18 or above is an attribute derived from the individual's date of birth.

7.2 Meaning of *restricted attribute* of an individual

For the purposes of paragraph 11(1)(f) of the Act, the following is prescribed as a restricted attribute:

(a) a number on a document or other credential listed in Schedules 1 to 4 that is a unique identifier for that particular version of the document or other credential.

Example: A card number on a driver's licence is a unique number for that particular version of the card and is in addition to the licence number on that card.

Part 7.2—Accreditation conditions

7.3 Table of accreditation conditions

For the purposes of subsection 17(5) of the Act, the accreditation of a kind of accredited entity specified in column 1 of an item of the following table is subject to the conditions specified in column 2 of the item in the circumstances (if any)specified in column 3 of the item.

Accreditation conditions

Item	Column 1 Entity	Column 2 Condition	Column 3 Circumstances
1	All accredited entities	Must not collect a restricted attribute of an individual unless the circumstances in column 3 exist:	where collection of the specific restricted attribute is authorised by an accreditation condition imposed by the: (a) the Digital ID Regulator under subsection 17(2) of the Act; or (b) an accreditation condition imposed by these rules. Note: an accreditation condition imposed on an entity under subitem 2(b) of Schedule 1 of Part 1 of the *Digital ID (Transitional and Consequential Provisions) Act 2023* is taken to have been imposed by the Digital ID Regulator under subsection 17(2) of the Act.
2	Accredited identity exchange provider	May collect a restricted attribute of an individual:	where the collection is for the purposes of the accredited identity exchange provider providing its accredited services to other participants in the digital ID system in which the entity operates or for a purpose specified in subsection 47(4) or paragraph 47(5)(a) of the Act. Note: An accredited identity exchange provider must not retain a restricted attribute of an individual (see section 56 of the Act).
3	Accredited identity service provider	May collect a restricted attribute of an individual that is on, or derived	

Accreditation conditions

Item	Column 1 Entity	Column 2 Condition	Column 3 Circumstances
		from, a credential provided by the individual.	
4	Accredited attribute service provider	May collect a restricted attribute of an individual: May collect a photo of the individual, or biometric information derived from the photo, on a document or other credential provided by the individual:	where the collection is for the purposes of using that restricted attribute or biometric information to verify the special attribute of the individual.
5	Accredited identity service provider	May collect biometric information that is an acquired image provided by the individual: May collect a photo of the individual, or information derived from the photo, on a document or other credential provided by the individual	where the collection is for the purposes of verifying the identity of the individual or authenticating the individual to their digital ID
6	Accredited identity service provider	May disclose s restricted attribute to an authoritative source, or to a service that confirms the veracity of an attribute or document or other credential with an authoritative source:	where the disclosure is for the purposes of verifying the identity of the individual
7	All accredited entities	May disclose restricted attributes or biometric information to a contractor engaged	where the disclosure is for the purposes of the contractor providing a service, or part of an accredited service, of the accredited entity and the contractor is contractually bound

Rule 7.3

Accreditation conditions			
Item	**Column 1** **Entity**	**Column 2** **Condition**	**Column 3** **Circumstances**
		by the accredited entity :	to comply with the same obligations applying to the accredited entity in respect of that information.
8	Accredited identity service provider:	May disclose passport numbers, driver's licence numbers, visa numbers, Australian proof of age card numbers and Medicare card numbers to a relying party that is a 'reporting entity' (within in the meaning of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006):*	where the disclosure of the passport number, driver's licence number, visa number, Australian proof of age card numbers or Medicare card number is for the purposes of the relying party complying with its obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

Part 7.3—Reportable incidents

7.4 General

This Part applies to an accredited entity when the entity is providing its accredited services in a digital ID system other than the Australian Government Digital ID System.

Note: The Digital ID Rules prescribe reportable incidents for accredited entities when providing accredited services in the Australian Government Digital ID System.

7.5 Reportable incidents

An accredited entity must notify the Digital ID Regulator within 5 business days if any of the following occurs:

(a) any material change in its circumstances that might affect its ability to comply with its obligations under the Act, these rules or the Accreditation Data Standards;

(b) any material change to the manner in which it provides its accredited services;

(c) any matter that could be relevant to a decision as to whether the entity is, having regard to the fit and proper person considerations referred to in section 12 of the Act, a fit and proper person to be accredited under the Act; or

(d) there is a change to, or the accredited entity becomes aware of an error in, any information provided to the Digital ID Regulator.

Note: For paragraph (c), see section 12 of the Act and the Digital ID Rules which prescribe matters to which the Digital ID Regulator must have regard when considering whether an entity is a fit and proper person.

7.6 Change of control for corporations

(1) In this rule:

corporation has the meaning given in the Corporations Act.

Corporations Act means the *Corporations Act 2001* (Cth).

director has the meaning given in section 9 of the Corporations Act and, for that purpose, body has the meaning given in that section.

officer has the meaning given in section 9 of the Corporations Act.

subsidiary has the meaning given in section 9 of the Corporations Act.

(2) For an accredited entity that is a corporation, the entity must notify the Digital ID Regulator, in accordance with this rule, of a change

in control (within the meaning of section 910B of the Corporations Act), or a proposed change of control.

(3) A notification of a change in control, or a proposed change of control, of an accredited entity must include the following information:

(a) the name of the incoming entity;

(b) the incoming entity's ABN or ARBN;

(c) the address of the incoming entity's principal place of business;

(d) if the incoming entity was incorporated outside Australia—the location of its incorporation and the address of its principal place of business in Australia;

(e) the date on which the incoming entity was registered under the Corporations Act or other law;

(f) the names and addresses of each of the directors and other officers of the incoming entity;

(g) in respect of each subsidiary of the incoming entity—the information specified in paragraphs (a) to (f) as if 'incoming entity' was replaced with 'the subsidiary'; and

(h) the date on which the change of control occurred or is proposed to occur.

(4) A notification required by this rule must be made:

(a) if the accredited entity becomes aware of a proposal for the change in control before it occurs—within 72 hours after the entity becomes aware; or

(b) otherwise—within 72 hours after the change in control occurs.

7.7 Entity no longer providing accredited services

If an accredited entity intends to cease providing accredited services, the entity must inform the Digital ID Regulator of its intent and details of its plans, as soon as practicable after forming that intent.

Note: Intent may arise where an accredited entity intends to sell, or otherwise dispose of, part of its business that includes provision of its accredited services.

Part 7.4—Data standards relating to accreditation

7.8 Digital ID Data Standards Chair to make standards

(1) For paragraph 99(1)(c) of the Act, the Digital ID Data Standards Chair must make standards, being one or more of technical, data or design standards relating to accreditation, on the matters specified in subsection (2).

(2) The matters are:

(a) authentication of individuals or information, including the kinds of authenticators and authentication levels to be bound to a digital ID;

(b) verification of information relating to an individual using biometric information of the individual;

(c) authenticating an individual to their digital ID using biometric information of the individual;

(d) test standards for an entity's information technology system involving the entity's biometric matching algorithm, including the testing metrics, evaluation and required minimum pass test results, and who may conduct the testing;

(e) test standards for an entity's information technology system involving the entity's technology for presentation attack detection, including the testing metrics, evaluation and required minimum pass test results, and who may conduct the testing.

Note: Accredited entities must comply with the Accreditation Data Standards applicable to the accredited service being provided and the manner of providing that service (see subparagraph 5.3(1)(a)(ii)).

Schedule 1—Documents or other credentials that are a commencement of identity credential

Note: See rule 1.4 (definition of 'commencement of identity credential') and subparagraph 5.2(1)(a)(iii) (requirement for verification of a document or other credential).

Item	Document of other credential used for verification:	must be verified by:
1	Birth certificate issued by a State or Territory government:	source verification.
3	Australian passport that is current or, if expired, no older than 3 years after the expiry date.	source verification; or technical verification.
4	Citizenship certificate—a notice given under section 37 of the *Australian Citizenship Act 2007* stating that a person is an Australian citizen at a particular time:	source verification.
5	Australian Certificate of Registration by Descent issued by the Australian Government:	source verification.
6	Visa	source verification, verified by a DVS (within the meaning of that term in section 15 of the *Identity Verification Services Act 2023*) using a current passport (including an ePassport) issued by a foreign country.
7	Certificate of Identity document issued by the Department of Foreign Affairs and Trade:	source verification.
8	Australian Document of Identity issued by the Department of Foreign Affairs and Trade:	source verification.
9	Convention Travel Document, also known as a *Titre de Voyage* issued by the Department of Foreign Affairs and Trade:	source verification.
10	ImmiCard issued to an individual, as a person who is not an Australian citizen, by the Department administered by the Minister administering the *Migration Act 1958* to assist the individual to prove the individual's identity:	source verification.

Schedule 2—Documents or other credentials that are a linking credential

Note: See rule 1.4 (definition of 'linking credential') and subparagraph 5.2(1)(a)(iii) (requirement for verification of a document or other credential).

Item	Document or other credential used for verification:	must be verified by:
1	Marriage certificate—a certificate of marriage issued by or on behalf of a State or Territory whose function it is to register marriages:	source verification.
2	Change of name certificate issued by or on behalf of a State or Territory indicating that an individual has changed the individual's name:	source verification.
3	Proof of divorce document, issued by a court, evidencing the dissolution of the individual's marriage:	source verification; or visual verification.
4	Victims' certificate issued under Division 375 of the *Criminal Code Act 1995* (Cth):	source verification; or visual verification.
5	Birth certificate issued by or on behalf of a State or Territory government:	source verification.

Schedule 3—Documents or other credentials that are a UitC credential

Note: See rule 1.4 (definition of 'UitC credential') and subparagraph 5.2(1)(a)(iii) (requirement for verification of a document or other credential).

Item	Credential used for verification:	must be verified by:
1	Concession or health care card issued by Services Australia:	source verification.
2	Medicare card (within the meaning of that term in Part VII of the *National Health Act 1953):*	source verification.
3	Student ID card issued by an: (a) Australian secondary school: (b) technical and further education institution (however described) operated by a State or Territory government: (c) Australian university; or (d) a registered training organisation (within the meaning of that term in the *National Vocational Education and Training Regulator Act 2011):*	source verification; or visual verification.
4	Statement issued by an authorised deposit-taking institution (within the meaning of that term in the *Banking Act 1959*) that : (a) contains the individual's current address; and (b) covers financial transactions in the previous 6 months before the statement is presented for the purposes of verification:	source verification; or visual verification.
5	Debit or credit card that is current and issued by an authorised deposit taking institution (within the meaning of that term in the *Banking Act 1959*):	source verification.
6	Certificate of education (however described) or certified academic transcript (an official transcript stamped and signed by the authorised officer of the education institute) issued by: (a) Australian secondary school: (b) technical and further education institution (however described) operated by a State or Territory government: (c) Australian university; or (d) a registered training organisation (within the meaning of that term in the *National Vocational Education and Training Regulator Act 2011):*	source verification; or visual verification.

Item	Credential used for verification:	must be verified by:
7	Veteran Card issued by the Department of Veterans' Affairs:	source verification; or visual verification.
8	Document evidencing registration of lease over real property and issued under a law of a State or Territory:	source verification; or visual verification.
9	Motor vehicle registration document showing proof of payment and the applicant's current address and issued under a law of a State or Territory:	source verification; or visual verification.
10	Rates notice issued under a law of a State or Territory and proof of payment where the notice: (a) is not more than 12 months old; and (b) contains the individual's current address:	source verification; or visual verification.
11	Document evidencing the individual's enrolment on the electoral roll maintained by the Australian Electoral Commission:	source verification.
12	Telephone records—document showing at least 6 months of phone usage and the individual's current residential address:	source verification; or visual verification.
13	Photo ID—a document or other credential listed in Schedule 4 but only if it has not already been used for the purposes of verification:	the verification requirements against that document or other credential in Schedule 4.
14	Utility account showing the individual's current residential address and which is no more than 6 months old:	source verification; or visual verification.
15	Superannuation statement showing the individual's current residential address and which is no more than 6 months old:	source verification; or visual verification.
16	Senior's card issued by or on behalf of a State or Territory:	source verification; or visual verification.
17	Land titles office record issued by or on behalf of a State or Territory:	source verification; or visual verification.
18	Insurance policy renewal where the individual is the insured and the policy has been held for more than 12 months:	source verification; or visual verification.

Schedule 4—Documents or other credentials that are a photo ID

Note: See rule 1.4 (definition of 'photo ID') and subparagraph 5.2(1)(a)(iii) (requirement for verification of a document or other credential).

Item	Documents of other credentials that contain a photo of the individual:	must be verified by:
2	Australian passport that is current or, if expired, no older than 3 years after the expiry date:	source verification; or technical verification.
3	Driver's licence issued under the law of a State or Territory:	source verification.
4	Foreign passport, other than an ePassport, issued by the government of a foreign country:	visual verification.
5	Foreign ePassport issued by the government of a foreign country:	technical verification.
6	Foreign military or defence force ID card—an identification card issued in the name of an individual by a foreign government showing a picture of the individual and identifying the individual as a current member of the military or defence forces of that government:	visual verification.
7	Convention Travel Document, also known as a *Titre de Voyage*, issued by the Department of Foreign Affairs and Trade:	source verification.
8	Citizenship certificate—a notice given under section 37 of the *Australian Citizenship Act 2007* stating that a person is an Australian citizen at a particular time:	source verification.
9	Shooter or firearms licence issued under a law of a State or Territory:	source verification; or visual verification.
10	Identity card issued for the purpose of the Aviation and Maritime Security Identification Card Schemes under the *Aviation Transport Security Act* 2004 or the *Maritime Transport and Offshore Facilities Security Act 2003:*	source verification.
11	Australian Government issued photo ID card (employee ID):	source verification; or visual verification.
12	Australian Department of Defence Highly Trusted Token:	source verification; or visual verification.
13	Defence Force identity card Issued by the Australian Defence Force:	source verification; or visual verification.
14	Police identity card:	source verification; or visual verification.
15	Trade or business licence such as a trade licence, real estate agent licence, security agents licence issued by or on behalf of a State or Territory:	source verification; or visual verification.

Item	Documents of other credentials that contain a photo of the individual:	must be verified by:
16	Tangentyere ID card issued by the Tangentyere Council Aboriginal Corporation, and which includes the individual's name and a photo of the individual:	source verification; or visual verification.
17	Proof-of-age card issued by or on behalf of a State or Territory:	source verification; or visual verification.
18	Working with children/vulnerable people card issued by or on behalf of a State or Territory:	source verification; or visual verification.

Schedule 5—PSPF controls

Note: See rule 4.3 (*Compliance with the PSPF*).

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 1	B.1		The accountable authority of each entity must:	a. determine their entity's tolerance for security risks
PSPF Policy 1	B.1			b. manage the security risks of their entity, and
PSPF Policy 1	B.1			c. consider the implications their risk management decisions have for other entities, and share information on risks where appropriate.
PSPF Policy 2	B.1		The accountable authority must:	a. appoint a Chief Security Officer (CSO) at the Senior Executive Service1 level to be responsible for security in the entity
PSPF Policy 2	B.1			b. empower the CSO to make decisions about: i. appointing security advisors within the entity ii. the entity's protective security planning iii. the entity's protective security practices and procedures iv. investigating, responding to, and reporting on security incidents

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 2	B.1			c. ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this
PSPF Policy 2		Requirement 1. Security advisors	The CSO must be responsible for directing all areas of security to protect the entity's people, information (including ICT) and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.	
PSPF Policy 2		Requirement 2. Security procedures	Entities must develop and use procedures that ensure:	a. all elements of the entity's security plan are achieved
PSPF Policy 2		Requirement 2. Security procedures		b. security incidents are investigated, responded to, and reported
PSPF Policy 2		Requirement 2. Security procedures		c. relevant security policy or legislative obligations are met.
PSPF Policy 2		Requirement 3. Security training	Entities must provide all personnel, including contractors, with security awareness training at engagement and annually thereafter.	
PSPF Policy 2		Requirement 4. Specific training	Entities must provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
			specific security awareness training targeted to the scope and nature of the position.	
PSPF Policy 2		Requirement 5. General email	Entities must maintain a monitored email address as the central conduit for all security-related matters across governance, personnel, information (including ICT) and physical security. Note: See the guidance advice in section C.9.4 of PSPF Policy 2 to assist in implementation of this requirement.	
PSPF Policy 3	B.1		Each entity must have in place a security plan approved by the accountable authority to manage the entity's security risks.	
PSPF Policy 3	B.1		The security plan details the:	a. security goals and strategic objectives of the entity, including how security risk management intersects with and supports broader business objectives and priorities
PSPF Policy 3	B.1			b. threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets
PSPF Policy 3	B.1			c. entity's tolerance to security risks
PSPF Policy 3	B.1			d. maturity of the entity's capability to manage security risks, and
PSPF Policy 3	B.1			e. entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 3		Requirement 2. Critical assets	Entities must identify people, information and assets that are critical to the ongoing operation of the entity and the national interest and apply appropriate protections to these resources to support their core business.	
PSPF Policy 3		Requirement 3. Risk steward	Entities must identify a risk steward (or manager) who is responsible for each security risk or category of security risk, including for shared risks.	
PSPF Policy 3		Requirement 5. Threat levels	The security plan (and supporting security plans) must include scalable measures to meet variations in threat levels and accommodate changes in the National Terrorism Threat Level.	
PSPF Policy 3		Requirement 6. Alternative mitigations	Where the CSO (or security advisor on behalf of the CSO) implements an alternative mitigation measure or control to a PSPF requirement, they must document the decision and adjust the maturity level for the related PSPF requirement.	
PSPF Policy 4	B.1		Each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan.	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 4		Requirement 1. Security maturity records	Entities must document and evidence their assessment of the entity's security maturity.	
PSPF Policy 6			Each entity is accountable for the security risks arising from procuring goods and services, and must ensure contracted providers comply with relevant PSPF requirements.	
PSPF Policy 6		Requirement 1. Assessing and managing security risks of procurement	When procuring goods or services, entities must put in place proportionate protective security measures by identifying and documenting:	a. specific security risks to its people, information and assets, and
		Requirement 1.		b. mitigations for identified risks.
PSPF Policy 6		Requirement 2. Establishing protective security terms and conditions in contracts	Entities must ensure that contracts for goods and services include relevant security terms and conditions for the provider to:	a. apply appropriate information, physical and personnel security requirements of the PSPF
PSPF Policy 6		Requirement 2.		b. manage identified security risks relevant to the procurement, and
PSPF Policy 6		Requirement 2.		c. implement governance arrangements to manage ongoing protective security requirements, including to notify the entity of any actual or suspected security incidents and

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
				follow reasonable direction from the entity arising from incident investigations.
PSPF Policy 6		Requirement 3. Ongoing management of protective security in contracts	When managing contracts, entities must put in place the following measures over the life of a contract:	a. ensure that security controls included in the contract are implemented, operated and maintained by the contracted provider and associated subcontractor, and
PSPF Policy 6		Requirement 3.		b. manage any changes to the provision of goods or services, and reassess security risks.
PSPF Policy 6		Requirement 4. Completion or termination of a contract	Entities must implement appropriate security arrangements at completion or termination of a contract.	
PSPF Policy 8			Each entity must:	a. identify information holdings
PSPF Policy 8				b. assess the sensitivity and security classification of information holdings, and
PSPF Policy 8				c. implement operational controls for these information holdings proportional to their value, importance and sensitivity.
PSPF Policy 8		Requirement 8. Transfer	Entities must ensure sensitive and security classified information is transferred and transmitted by means that deter and detect compromise and that meet the minimum protection requirements set out in Annexes A to D.	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 8		Requirement 9. Disposal	Entities must ensure sensitive and security classified information is disposed of securely in accordance with the minimum protection requirements set out in Annexes A to D. This includes ensuring sensitive and classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.	
PSPF Policy 9	B.1		Each entity must enable appropriate access to official information. This includes:	a. sharing information within the entity, as well as with other relevant stakeholders
PSPF Policy 9	B.1			b. ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information, and
PSPF Policy 9	B.1			c. controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.
PSPF Policy 9		Requirement 5. Managing access to information systems	To manage access to information systems holding sensitive or security classified information, entities must implement unique individual identification, authentication and authorisation practices on each occasion where system access is granted.	
PSPF Policy 11	B.1		Each entity must ensure the secure operation of their ICT systems to safeguard their information and data and the continuous	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
			delivery of government business by applying the Information Security Manual's cyber security principles during all stages of the lifecycle of each system.	
PSPF Policy 11		Requirement 1. Authorisation of ICT systems to operate	Entities must only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation.	
PSPF Policy 11		Requirement 1. Authorisation of ICT systems to operate	Entities must only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation. When establishing new ICT systems, or implementing improvements to an existing system, the decision to authorise (or reauthorise) a system to operate must be based on the ISM's six step risk-based approach for cyber security.	
PSPF Policy 11		Requirement 4. Vulnerability Disclosure Program	Entities must have in place a vulnerability disclosure program.	
PSPF Policy 12	B.1		Each entity must ensure the eligibility and suitability of its personnel who have access	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
			to Australian Government resources (people, information and assets).	
PSPF Policy 12		Requirement 1. Pre- employment screening	Entities must undertake pre-employment screening, including:	a. verifying a person's identity using the Document Verification Service
PSPF Policy 12		Requirement 1.		c. obtaining assurance of a person's suitability to access Australian Government resources, including their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm.
PSPF Policy 13	B.1		Each entity must assess and manage the ongoing suitability of its personnel and share relevant information of security concern, where appropriate.	
PSPF Policy 14	B.1		Each entity must ensure that separating personnel:	a. have their access to Australian Government resources withdrawn, and
PSPF Policy 14	B.1			b. are informed of any ongoing security obligations.
PSPF Policy 14		Requirement 1. Sharing security relevant information, debriefs and continuing obligations	Prior to personnel separation or transfer, entities must:	a. notify the Chief Security Officer, or relevant security advisor, of any proposed cessation of employment resulting from misconduct or other adverse reasons

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 14		Requirement 2. Withdrawal of access	On separation or transfer, entities must remove personnel's access to Australian Government resources, including:	a. physical facilities, and
PSPF Policy 14		Requirement 2.		b. ICT systems.
PSPF Policy 14		Requirement 3. Risk assessment	Where it is not possible to undertake required separation procedures, entities must undertake a risk assessment to identify any security implications.	
PSPF Policy 15			Each entity must implement physical security measures that minimise or remove the risk of:	a. harm to people, and
PSPF Policy 15				b. information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
PSPF Policy 15		Requirement 1. Physical security measures	Entities must put in place appropriate physical security measures to protect entity resources, commensurate with the assessed business impact level of their compromise.	
PSPF Policy 15		Requirement 2. Security containers, cabinets and rooms	Entities must assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 15		Requirement 3. Disposal	Entities must dispose of physical assets securely.	