Digital ID (Accreditation) Rules 2024

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

Dated 7 November 2024

Katy Gallagher
Minister for Finance

Contents

Chapter 1—Preliminary

1.1 Name

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

1.2 Commencement

These rules commence at the same time as the *Digital ID Act 2024* commences.

1.3 Authority

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

1.4 Definitions

Note: A number of expressions used in these rules are defined in the Act, including the following:

(a) accredited entity;
(b) attribute;
(c) digital ID;
(d) participating relying party;
(e) personal information.

Note 2: A number of expressions used in these rules are defined in the Accreditation Data Standards, including the following:

(a) AL Table;
(b) authentication level;
(c) in-device biometric capability;
(d) out-of-band device.

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

(2) In these rules:

accessibility and useability assessment means an assessment conducted in accordance with 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, proposed accredited services and accredited services.

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.

Rule 1.4

Act means the *Digital ID Act 2024*.

alternative proofing process: see rule 5.22.

annual review: see rule 6.1.

applicant: see rule 1.9.

approved cryptography means:

(a) Australian Signals Directorate Approved Cryptographic Algorithms; and

(b) Australian Signals Directorate Approved Cryptographic Protocols,

as each is defined either in the ISM or the document *Implementing Certificates, TLS, HTTPS and Opportunistic TLS* published by the Australian Signals Directorate.

Note: At the time these rules were made, located at https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Implementing%20Certificates%2C%20TLS%2C%20HTTPS%20and%20Opportunistic%20TLS%20%28October%202021%29.pdf.

ASP means an accredited attribute service provider.

assessing officer means a member of personnel of an applicant or 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.

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

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

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 IP2 Plus, IP3 or IP4.

Note: See item 4 of the IP Levels Table.

biometric capability, in relation to an applicant or accredited entity, means the components of the 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.

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

Note: A commencement of identity credential 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, proposed accredited services 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 applicant or accredited entity.

DI data environment means digital ID data environment.

digital ID data environment means the information technology systems used for, and the processes that relate to:

(a) for an applicant—the provision of the entity's proposed accredited services; or

(b) for an accredited entity—the entity's accredited services.

Digital ID Rules means the *Digital ID Rules 2024*.

eIDVT means electronic identity document verification technology that uses non-cryptographic techniques to classify physical documents or other credentials submitted online by an individual as being genuine or not genuine.

eIDVT biometric matching means biometric matching that uses a facial image acquired from a photo ID that has been classified as a genuine document by eIDVT to match against an acquired image.

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 means an assessment conducted in accordance with rule 3.6.

fraud control plan: see rule 4.31.

fraud controller: see rule 4.27.

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: an entity holds personal information if the entity has possession or control of a record that contains the personal information.

Rule 1.4

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 or ***IP level*** means a level specified in the first row of the IP Levels Table.

image quality profile means the profile that captured biometric information is compared against to ensure that it meets a threshold for information quality before being used for biometric binding or authentication.

IP Levels Table means the table in rule 5.10.

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).

ISO/IEC 29794-5 means Part 5 (concerning face image data) of the series of standards designated ISO/IEC 29794 (concerning biometric sample quality), published by the International Organization for Standardization.

Note: At the time this instrument was made, the current version was ISO/IEC TR 29794-5:2010, located at https://www.iso.org/standard/50912.html.

ISO/IEC 27001 means the standard for information security management systems, published by the International Organization for Standardization.

Note: At the time this instrument was made, the current version was ISO/IEC 27001:2022, located at https://www.iso.org/standard/27001.

ISO/IEC 30107-1 means Part 1 (concerning framework) of the series of standards designated ISO/IEC 30107 (concerning biometric presentation attack detection), published by the International Organization for Standardization.

Note: At the time this instrument was made, the current version was ISO/IEC 30107-1:2023, located at https://www.iso.org/standard/83828.html.

ISO/IEC 24745 means the standard for information security, cybersecurity and privacy protection, published by the International Organization for Standardization

Note: At the time this instrument was made, the current version was ISO/IEC 24745:2022, located at https://www.iso.org/standard/75302.html.

ISP means an accredited identity service provider.

IXP means an accredited identity exchange provider.

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 if that individual's attributes have changed.

liveness detection means the measurement and analysis of biometric, biological and behavioural characteristics or involuntary or voluntary reactions of the live presentation of an individual, in order to determine if a biometric sample is being captured from a living individual who is physically present at the place and time when the biometric sample is captured.

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

material change, in relation to an entity, means any change that alone or cumulatively results in, or is reasonably likely to result in:

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

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

Note: The definition of 'material change' in these rules is different to the definition of the same expression in the Digital ID Rules.

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

penetration testing means testing conducted in accordance with Division 1 of Part 3.3 of Chapter 3.

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 proposed accredited services or accredited services.

photo ID means a document or other credential listed in Schedule 4.

physical authenticator: see rule 5.25.

presentation attack means the presentation of an artefact to a biometric data capture subsystem with the goal of interfering with the expected operation of the biometric capability.

presentation attack detection means automated discrimination between bona-fide presentations and presentation attacks.

presentation attack instrument means an object or biometric characteristic that is used in a presentation attack.

Privacy Act means the *Privacy Act 1988*.

proposed accredited services, in relation to an applicant, means the services proposed to be provided by the entity in its application under section 14 of the Act for accreditation as an accredited entity.

protective security assessment means an assessment conducted in accordance with Division 1 of Part 3.2 of Chapter 3.

protective security capability: see Division 1 of Part 4.1 of Chapter 4.

protective security framework: see Division 2 of Part 4.1 of Chapter 4.

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 proposed accredited services, in relation to an applicant, means the proposed accredited services or elements of the entity's information technology system that an individual directly interacts with when using, or attempting to use, the entity's proposed accredited services.

public-facing accredited services, in relation to an accredited entity, means the accredited services or elements of the 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 ISP's mobile app that the individual is required to download so as to access the entity's accredited services.

public-facing information related to proposed accredited services, in relation to an applicant, means information made available by the entity to individuals when interacting with the entity's public-facing proposed accredited services.

public-facing information related to accredited services, in relation to an accredited entity, means information made available by the 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 rule 6.1.

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.

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 5.32.

Note: An ASP 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 that lists:

(a) for an applicant:

(i) each requirement in these rules and the Accreditation Data Standards with which the entity must comply in relation to its proposed accredited services if accredited; and

(ii) the evidence that demonstrates the entity will comply with those requirements if accredited; or

(b) for an accredited entity:

(i) each requirement in these rules and the Accreditation Data Standards with which the entity must comply in relation to its accredited services; and

(ii) the evidence that demonstrates the entity complies with those requirements.

system security plan: see rule 4.12.

systems testing means penetration testing, useability testing or WCAG testing.

taking reasonable steps: see rule 1.5.

technical biometric matching means the process of verifying that an acquired image biometrically matches the image of the individual 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.

transitioned accredited entity means an entity taken to be accredited immediately after commencement of the Act in accordance with item 2 of Schedule 1 to the *Digital ID (Transitional and Consequential Provisions) Act 2024*.

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.

useability testing means testing conducted in accordance with Division 2 of Part 3.3 of Chapter 3.

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 2.1 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'.

WCAG testing means testing conducted in accordance with Division 3 of Part 3.3 of Chapter 3.

1.5 Meaning of *taking reasonable steps*

In these rules, ***taking reasonable steps***, in relation to a duty to ensure an identified outcome, means taking 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.

1.6 Meaning of *authenticated session*

For the purposes of subsection 56(3) of the Act:

authenticated session means a persistent interaction between 2 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.

1.7 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 to the incorporated instrument has taken effect.

Note: See subsection 167(3) of the Act.

(3) Subrule (2) does not apply if the incorporated instrument is an Act or a legislative instrument.

1.8 Application—transitioned accredited entities

(1) A provision in column 1 of an item in the following table applies to a transitioned accredited entity starting on the day that is 12 months after the day on which these rules commence, subject to the exception (if any) in column 2 of that item.

Application of these rules to transitioned accredited entities

Item	Column 1 Provision	Column 2 Exception
1	rule 4.14	
2	rule 4.19	
3	subrules 4.20(3) and (4)	
4	paragraph 4.22(2)(b)	
5	subrule 4.38(3)	The requirements in relation to privacy policies in this subrule apply to a transitioned accredited entity on and from the commencement of these rules.
6	subrule 4.41(3)	
7	subrule 4.42(2)	
8	paragraph 4.50(3)(c) and subrules 4.50(4), (5) and (6)	
9	rule 4.51	
10	rule 5.2	
11	rule 5.7	
12	subrule 5.9(2)	

(2) Every provision of these rules not specified in subrule (1) applies to a transitioned accredited entity in accordance with its terms and on and from the commencement of these rules.

Rule 1.9

1.9 Application—applicants

(1) These rules apply to an entity (an ***applicant***):

(a) that has made an application under section 14 of the Act for accreditation as an accredited entity; and

(b) at the time the entity applies for such accreditation.

(2) These rules apply to, and in relation to, an applicant with the modifications in this rule.

(3) If, because of Chapter 2 and subrule (4):

(a) an applicant is required to implement any measure in accordance with, or comply with, a provision in Chapter 3, 4 or 5 of these rules, or a provision in the Act or Accreditation Data Standards—the applicant must implement that measure in accordance with, or comply with, that provision as if the applicant is an accredited entity that is accredited to provide its proposed accredited services; and

(b) the ability or capacity of an applicant to implement any measure in accordance with, or comply with, a provision in Chapter 3, 4 or 5 of these rules, or a provision in the Act or Accreditation Data Standards, is to be assessed—the assessment is to be undertaken as if the applicant were an accredited entity that is accredited to provide its proposed accredited services.

(4) For the purposes of Chapter 2, an expression in column 1 of an item in the following table that appears in Chapter 3, 4 or 5 of these rules, or in a provision of the Act or Accreditation Data Standards, applies to, or in relation to, an applicant subject to the modification in column 2 of that item.

Application of these rules to applicants

Item	Column 1 Expression	Column 2 Modification
1	accredited entity	to be taken as a reference to an applicant.
2	accredited services	to be taken as a reference to proposed accredited services.
3	ASP	to be taken as a reference to an applicant who has applied to be an ASP.
4	digital ID fraud incident	to be taken to include an act, event or circumstance that occurs in connection with a proposed accredited service of an applicant and results in any of the circumstances in paragraph (b) of the definition of 'digital ID fraud incident' in section 9 of the Act.
5	ISP	to be taken as a reference to an applicant who has applied to be an ISP.
6	IXP	to be taken as a reference to an applicant who has applied to be an IXP.
7	public-facing accredited services	to be taken as a reference to public-facing proposed accredited services.

Application of these rules to applicants		
Item	**Column 1** **Expression**	**Column 2** **Modification**
8	public-facing information related to accredited services	to be taken as a reference to public-facing information related to proposed accredited services.

Rule 2.1

Chapter 2—Applying for accreditation

2.1 DI data environment

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

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

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

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

(b) has limited the boundaries of its DI data environment to the extent practicable, including by:

(i) segregating 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 made by an applicant 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(2) are met; and

(iii) if a cloud service provider has conducted penetration testing as required by paragraph 3.8(4)(a)—the applicant 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 paragraph 2.3(3)(e), copy of reports of the testing and any required responses to the reports.

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 must meet the criteria in this rule.

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

(3) The applicant must, at the time it applies for accreditation, have conducted:
- (a) assurance assessments in accordance with Chapter 3;
- (b) systems testing in accordance with Chapter 3;
- (c) a privacy impact assessment in accordance with rule 2.4;
- (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;
- (f) a cyber security risk assessment in accordance with rule 4.7; and
- (g) a fraud risk assessment in accordance with rule 4.25.

2.4 Privacy impact assessment

(1) The applicant must, at the time it applies for accreditation, have conducted 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 identified, defined, documented and limited in accordance with 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 proposed 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 compliance with the privacy requirements specified in Chapter 3 of the Act and Part 4.3 of Chapter 4 of these rules;
  - (iii) an analysis of how the applicant's provision of its proposed accredited services will impact the privacy of individuals and protection of personal information, if the applicant is accredited, including how the applicant will comply with any applicable requirements in Chapter 5 of these rules and the Accreditation Data Standards;

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

(v) any recommendations made by the person who conducted the assessment, including recommendations that the applicant undertake activities to mitigate any identified privacy risks;

(vi) 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 actions to address such risks or recommendations are not necessary; and

(vii) 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 or recommendation identified by 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 the risk matrix developed in accordance with paragraph (a);

(d) respond to each risk identified in the report with actions it will take to address the risk; and

(e) respond to each recommendation in the assessment.

(6) The applicant's response to each risk needing to be addressed and each recommendation must include:

(a) for each risk or recommendation that the applicant will address:

(i) details of the action the applicant will take to address the risk 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 that the applicant will not address:

(i) the reasons for the applicant's decision not to address the risk;

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

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

2.5 Technical testing

(1) The applicant must, at the time it applies for accreditation, have conducted technical testing in accordance with this rule.

(2) The technical testing of the information technology system through which the applicant will provide its accredited services must determine whether the system has the functionality necessary to meet the following requirements:

(a) incident monitoring, detection, investigation, management and response for cyber security incidents as required by Subdivision C of Division 3 of Part 4.1 of Chapter 4;

(b) logging requirements as required by rule 4.20;

(c) incident monitoring, detection, investigation, management and response for fraud incidents as required by Division D of Part 4.2 of Chapter 4;

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

(e) data minimisation requirements, as required by subrule 4.42(2); and

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

(3) The applicant 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) how each test maps to each requirement referred to in subrule (2); and

(e) the results of the technical testing, including details of any failure to meet the requirements in subrule (2) that is identified and how this failure has been addressed.

2.6 Matters to which the Digital ID Regulator must have regard

(1) For the purposes of paragraph 15(5)(a) of the Act, in deciding whether to accredit an applicant, the Digital ID Regulator must have regard to the following matters:

(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 proposed accredited services to be provided by the entity 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 proposed accredited services to be provided by the entity if accredited; and

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

(2) This rule is not limited by paragraph 1.9(3)(b).

2.7 Matters of which the Digital ID Regulator must be satisfied

(1) For the purposes of paragraph 15(4)(d) of the Act, the Digital ID Regulator must not accredit an applicant unless it is satisfied that the information and documents provided by the applicant demonstrate that the applicant, if accredited, will be able to comply with:

(a) the Act;

(b) these rules; and

Rule 2.7

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

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 5.1(1)(a)(ii)).

(2) This rule is not limited by paragraph 1.9(3)(b).

Chapter 3—Assurance assessments and systems testing

Part 3.1—General requirements

3.1 Entity's obligation

(1) If an accredited 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 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 accredited entity must comply as detailed in the entity's statement of scope and applicability; and

(b) in respect of the entity'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 (***assessor***):

(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 requested by the assessor, an accredited 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, in relation to an accredited entity:
  (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 of Chapter 4, or ability to comply if accredited;
  (b) review and address the results of the penetration testing report referred to in rule 3.10;
  (c) review and address any findings or recommendations in the entity's report of its essential strategies review referred to in paragraph 3.4(2)(b); and
  (d) if the entity considers a control or strategy is not relevant to the entity—comply with the requirements of rule 3.5.

(2) 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 accredited 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 accredited entity's DI data environment or accredited services.

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

3.4 Essential strategies review and report

(1) In this rule:

Essential Eight Maturity Model and ISM Mapping document means the document titled 'Essential Eight Maturity Model and ISM Mapping' 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-maturity-model-ism-mapping.

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 accredited entity must:

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

(b) provide a report to the assessor (***essential strategies report***).

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

(4) An essential strategies report must be in the form of the assessment report template in the Essential Eight Assessment Process Guide and must include the following information:

(a) the opinion of the person conducting the review as to whether the accredited entity has implemented and complies with the maturity level 2 controls specified in the ISM;

(b) if an accredited 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 any recommendations on the accredited entity's compliance with the Essential Eight Maturity Model and ISM Mapping document for ISM controls marked maturity level 2.

3.5 If a control or strategy is not relevant to an accredited entity

(1) If an accredited entity considers that a particular protective security control in the framework it implements or strategy in rule 4.19 is not relevant to the entity, and has not or does not intend to implement that control or strategy, the entity must:

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

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

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

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

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

(iii) whether the entity's decision that a particular control or strategy is not relevant to it is appropriate.

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 or strategy is not relevant to the accredited entity, the control must be implemented.

Rule 3.6

Division 2—Fraud assessment

3.6 Requirements

(1) A fraud assessment must review and assess:

(a) an accredited entity's implementation and compliance with the fraud control requirements in Part 4.2 of Chapter 4; and

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

(2) An assessor conducting a fraud assessment must:

(a) be external to the accredited 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 accredited 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) of the Act.

(2) An accessibility and useability assessment must, in relation to an accredited entity, review and assess:

(a) the entity's compliance with subsection 30(1AA) of the Act;

(b) the entity's implementation and compliance with rule 4.49;

(c) for an ISP—the entity's implementation and compliance with the additional accessibility and useability requirements in Division 4 of Part 5.1 of Chapter 5;

(d) the findings of the WCAG testing, including actions that will address any risks and recommendations identified in the assessor's report of the WCAG testing; and

(e) if the entity is required to conduct useability testing—the findings of the useability testing, including actions that will address any risks and recommendations identified in the assessor's report of the useability testing.

Rule 3.8

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 accredited entity provides, or will provide, its accredited services by emulating the tools and techniques of likely attackers to exploit security weaknesses.

(2) 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) If an accredited entity uses the 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) must 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 accredited entity's arrangement with a cloud service provider does not allow penetration testing by the entity of the cloud service provider's infrastructure:
  (a) the entity must ensure the cloud service provider has conducted the kinds of penetration testing referred to in subrule (2) on that infrastructure at least once in each of the accredited entity's reporting periods; and
  (b) the requirements in rules 3.9 and 3.10 do not apply to penetration testing conducted by the cloud service provider.

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

Applicants

(6) If subrule (4) applies to an applicant because of rule 2.3, the words 'at least once in each of the accredited entity's reporting periods' appearing in paragraph 4(a) are to be ignored.

3.9 Penetration testing assessor

Penetration testing must be conducted by an assessor who meets the following additional requirements:
  (a) be external to the accredited 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 accredited entity's DI data environment or accredited services.

3.10 Penetration testing report

An assessor that has completed penetration testing for an accredited entity must prepare a report of that testing that includes:

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

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

(c) the results of the penetration testing, including:

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

(ii) any other findings; and

(iii) any recommendations.

Division 2—Useability testing

3.11 Accessible and inclusive services

This Division applies for the purposes of subsection 30(1) of the Act.

3.12 Useability testing requirements

(1) Useability testing of an accredited entity's public-facing accredited services must:
  (a) identify any adverse 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) include testing of all user interfaces an individual will progress through when interacting with the accredited entity's public-facing accredited services and, if applicable:
    (i) each interface involving verification or authentication in relation to an individual;
    (ii) alternative channels (if any) available to the individual to complete a specific activity;
    (iii) notices in relation to privacy, including notices or information required to be given to individuals in respect of privacy matters; and
    (iv) any other information required by these rules to be given to individuals;
  (b) involve a diverse range of individuals covering diversity in disability, age, gender and ethnicity; and
  (c) 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.

Note: Paragraph (2)(b) is made, in relation to accredited entities, for the purposes of paragraph 30(2)(c) of the Act. Paragraph (2)(c) is made, in relation to accredited entities, for the purposes of paragraph 30(2)(d) of the Act.

3.13 Useability testing report

An assessor that has completed useability testing of an accredited entity's public-facing accredited services must prepare a useability testing report that includes:
  (a) a description of the scope of testing;
  (b) a description of the tools and processes used to conduct the testing;
  (c) the results of the testing, including:
    (i) findings and qualitative metrics; and
    (ii) identification of any accessibility or useability issues; and
  (d) recommendations to address any accessibility or useability issues involving the accredited entity's accredited services.

Division 3—WCAG testing

3.14 Accessible and inclusive services

This Division applies for the purposes of subsection 30(1) of the Act.

3.15 WCAG testing requirements

WCAG testing must test the extent to which an accredited entity's:

(a) public-facing information related to accredited services on its web pages (within the meaning of that term in the WCAG) satisfies the Level A Success Criteria specified in WCAG version 2.1 in accordance with subrule 4.49(2); and

(b) public-facing accredited services and public-facing information related to accredited services satisfy the Level AA Success Criteria specified in WCAG version 2.1 in accordance with subrule 4.49(3).

3.16 WCAG testing report

An assessor that has conducted WCAG testing must prepare a WCAG testing report that includes:

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

(b) a description of the tools and processes used to test the compliance of the accredited entity's public-facing accredited services and public-facing information related to accredited services with the requirements in rule 3.15; and

(c) the results of the WCAG testing, including:

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

(ii) any other findings; and

(iii) any recommendations.

Rule 3.17

Part 3.4—Reports for assurance assessments and systems testing

3.17 Assessor's report

Without limiting rules 3.4, 3.10, 3.13 and 3.16, 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 any 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 actions the accredited entity should take to address the risk; and

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

(2) The accredited 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 accredited entity 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 the risk matrix developed in accordance with paragraph (a);

(d) respond to each risk identified in the report with actions it will take to address the risk; and

(e) respond to each recommendation in the report.

(4) The accredited entity's response to each risk needing to be addressed and each recommendation must include:

(a) for each risk or recommendation that the entity will address:

(i) details of the action the entity will take to address the risk 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 or recommendation that the entity will not address:

(i) the reasons for the entity's decision not to address the risk;

(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 completion 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 the protective security of its DI data environment 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 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

An accredited entity must implement, in respect of its accredited services and DI data environment, one of the following:

(a) the PSPF, subject to the requirements in rule 4.3;
(b) ISO/IEC 27001, subject to the requirements in rule 4.4;
(c) an alternative framework, subject to the requirements in rule 4.5.

4.3 Compliance with the PSPF

(1) If an accredited entity implements the PSPF for the purpose of rule 4.2, the entity must comply with, and manage and monitor, each of the controls specified in that framework that are listed in Schedule 5.

(2) Subrule (1) applies subject to rule 4.6.

(3) For the purposes of these rules:
(a) the term 'sensitive information' used in the PSPF has the same meaning as 'personal information' in the Act;
(b) the term 'Australian Government resources' used in the PSPF has the same meaning as 'DI data environment' in these rules;
(c) the term 'risks' in the PSPF has the same meaning as 'cyber security risks' in these rules.

(4) In Schedule 5:

B.1 and ***B.1 Core requirement***, in relation to a particular policy of the PSPF, mean the core requirement designated 'B.1' in that policy.

B.2 Supporting requirement, in relation to a particular policy of the PSPF, means the supporting requirement designated 'B.2' in that policy.

PSPF Policy 1 means Policy 1 (*Role of accountable authority*) of the PSPF.

PSPF Policy 2 means Policy 2 (*Management structures and responsibilities*) of the PSPF.

PSPF Policy 3 means Policy 3 (*Security planning and risk management*) of the PSPF.

PSPF Policy 4 means Policy 4 (*Security maturity monitoring*) of the PSPF.

PSPF Policy 6 means Policy 6 (*Security governance for contracted goods and service providers*) of the PSPF.

PSPF Policy 8 means Policy 8 (*Classification system*) of the PSPF.

PSPF Policy 9 means Policy 9 (*Access to information*) of the PSPF.

PSPF Policy 11 means Policy 11 (*Robust ICT systems*) of the PSPF.

PSPF Policy 12 means Policy 12 (*Eligibility and suitability of personnel*) of the PSPF.

PSPF Policy 13 means Policy 13 (*Ongoing assessment of personnel*) of the PSPF.

PSPF Policy 14 means Policy 14 (*Separating personnel*) of the PSPF.

PSPF Policy 15 means Policy 15 (*Physical security for entity resources*) of the PSPF.

Senior Executive Service has the same meaning as in the *Public Service Act 1999*.

Note: At the time these rules were made, all policies comprising the PSPF were located at https://www.protectivesecurity.gov.au/.

4.4 Compliance with ISO/IEC 27001

(1) If an accredited entity implements ISO/IEC 27001 for the purpose of subrule 4.2, the entity must comply with, and manage and monitor, all the controls specified in that standard.

(2) Subrule (1) applies subject to rule 4.6.

(3) For the purposes of these rules:
  (a) the term 'Personally Identifiable Information' used in ISO/IEC 27001 has the same meaning as 'personal information' in the Act;
  (b) the term 'information security incident' used in ISO/IEC 27001 has the same meaning as 'cyber security incident' in the Act; and
  (c) the term 'information security risk' used in ISO/IEC 27001 has the same meaning as 'cyber security risk' in these rules.

4.5 Implementation and compliance with an alternative framework

(1) An accredited entity may only implement an alternative framework if the entity demonstrates, in accordance with subrule (2) or (3), that the entity complies with all the same kinds of controls that would be required by either:
  (a) rule 4.3, if the entity were to implement the PSPF for the purpose of rule 4.2; or
  (b) rule 4.4, if the entity were to implement ISO/IEC 27001 for the purpose of rule 4.2.

(2) To demonstrate that the accredited entity complies with all the same kinds of controls as the PSPF for the purpose of paragraph (1)(a), the accredited entity must prepare and maintain an up-to-date document that:
  (a) maps all the controls specified in the alternative framework that must be complied with against the corresponding controls mentioned in rule 4.3; and
  (b) if the alternative framework does not require compliance with a particular kind of control mentioned in rule 4.3—specifies the relevant control mentioned in that rule.

(3) To demonstrate that the accredited entity complies with all the same kinds of controls as ISO/IEC 27001 for the purpose of paragraph (1)(b), the accredited entity must prepare and maintain an up-to-date document that:

(a) maps all the controls specified in the alternative framework that must be complied with against the corresponding controls mentioned in rule 4.4; and

(b) if the alternative framework does not require compliance with a particular kind of control mentioned in rule 4.4—specifies the relevant control mentioned in that rule.

(4) If an accredited entity implements an alternative framework for the purposes of rule 4.2, the entity must:

(a) continue to comply with, and manage and monitor:

(i) all the controls specified in that framework; and

(ii) any controls specified in the document prepared and maintained in accordance with paragraph (2)(b) or (3)(b); and

(b) comply with a new version of the alternative framework within the timeframe specified for that version.

(5) For the purpose of paragraph (4)(b), if a new version of the framework does not specify a timeframe for compliance, the timeframe for compliance is taken to be 12 months.

(6) Subrule (4) applies subject to rule 4.6.

4.6 If 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.

Rule 4.7

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) The accredited entity must:
  (a) develop a risk matrix based on an established risk management framework or standard; and
  (b) as part of the cyber security risk assessment:
    (i) assess the entity's cyber security risks in accordance with the risk matrix developed in accordance with paragraph (a);
    (ii) record the results of the assessment;
    (iii) determine and record the entity's level of tolerance to cyber security risks; and
    (iv) record how the entity's controls for cyber security risks are applied to its accredited services and DI data environment.

(3) If an ISP collects, uses, holds, discloses or destroys biometric information, the ISP must assess and record in its cyber security risk assessment the security risks, mitigation strategies and any other actions the ISP will take to address risks related to biometric information.

Applicants

(4) If subrule (1) applies to an applicant because of rule 2.3, the words 'for each reporting period' appearing in that subrule are to be ignored.

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 as 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 (*Ongoing assessment of personnel*). At the time these rules were made, located at https://www.protectivesecurity.gov.au/.

4.10 Advice to individuals

An ISP must provide advice to individuals about how to safeguard their digital ID against cyber security risks and update that advice, as soon as practicable, as new risks and threats emerge.

4.11 Support to individuals

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

(2) For the purposes of subrule (1), support services must include, at a minimum, the provision of:

(a) one of the following:

(i) a monitored chat function; or

(ii) a monitored email function; or

(iii) a call centre; and

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

Rule 4.12

Subdivision A—System security plan

4.12 Requirements for system security plan

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

(2) 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 (*Robust ICT systems*); and
  (b) must contain any other information required by these rules to be in the system security plan.

Note: At the time these rules were made, PSPF Policy 11 (*Robust ICT systems*) was located at https://www.protectivesecurity.gov.au/.

(3) 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.

Goals and strategic objectives

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

Destruction of biometric information

(5) If an ISP collects biometric information, the ISP'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) If another person collects biometric information from, or on behalf of, an ISP, the ISP's system security plan must include details of the arrangements in place for the other person 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 ISP.

Assessment of risks related to biometric information

(7) If an ISP collects, uses, holds, discloses or destroys biometric information, the ISP's system security plan must include details of any cyber security risks, associated mitigation strategies and any other actions the ISP will take to address risks 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) 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; and
(e) potential and known threats and attacks to the entity's biometric capability;

Use of out-of-band authenticators via PSTN

(8) If an ISP 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 address those risks.

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 each reporting period; and
(b) as soon as practicable after:
(i) the entity becomes aware of any 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 for cyber security risks;
(ii) the entity becomes aware of any breach of a requirement specified in its system security plan; or
(iii) any change in the entity's organisational structure or control, functions or activities, if that change will, or is reasonably likely to, increase the level of cyber security risk.

(2) The entity's review of its system security plan must, at a minimum:
(a) have regard to any 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, if necessary, update the goals and strategic objectives in the entity's system security plan, including:
(i) recording whether each goal and strategic objective has been met; and
(ii) updating the goals and strategic objectives for the next year.

Note: If the entity implements the ISO/IEC 27001, 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 the entity has completed each review of its system security plan, the entity must make all necessary amendments to its system security plan.

Rule 4.14

Subdivision B—Cloud service management

4.14 Selection, use and management of cloud services

(1) If 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 protective security controls and strategies that must be complied with in accordance with the Act, these rules and the Accreditation Data Standards in relation to the entity's use of cloud services;
  (c) periodic penetration testing and assurance assessments for the effectiveness of the protective security controls and strategies mentioned in paragraph (b), including in relation to:
    (i) geographic location;
    (ii) management of privileged access; and
    (iii) effective destruction of data;
  (d) responding to cyber security incidents or suspected cyber security incidents involving cloud services;
  (e) the orderly migration of information to and from cloud services;
  (f) monitoring, reviewing and evaluating the ongoing use of cloud services to manage cyber security risks;
  (g) if personal information is to be collected, held, used or disclosed using cloud services;
    (i) how that information will be collected, held, used or disclosed; and
    (ii) how personal information will be destroyed once it is no longer required; and
  (h) 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 whose services it uses which includes the following information:
  (a) the cloud services provider's name and cloud service name;
  (b) the entity's purpose for using the cloud services;
  (c) the type of personal information collected, used, held or disclosed by the cloud services provider (if any);
  (d) the date for the next protective security assurance assessment of the cloud services;
  (e) contractual arrangements for the use of the cloud service by the entity; 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 C—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 entities to report actual or suspected cyber security incidents to the accredited entity on a confidential basis.

4.16 Incident investigation, management and response

(1) An accredited entity must implement and maintain mechanisms for investigating and dealing with cyber security incidents which relate 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;
  (b) for an ISP:
    (i) identify any digital ID that has been affected by a cyber security incident; and
    (ii) suspend and prevent use of the digital ID; and
  (c) for an ASP:
    (i) identify any special attributes that have been affected by a cyber security incident; and
    (ii) suspend and 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 members of the entity's personnel who perform recovery tasks such as backup recovery and restoration;
  (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 any other plans in respect of its other business or organisational functions.

(3) An accredited entity must, 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

(1) This rule applies to cyber security incidents that cause, or are likely to cause, serious harm to one or more individuals.

(2) An accredited entity must prepare and keep records of:
  (a) any 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 a cyber security incident.

(3) For each reporting period, an accredited entity must prepare a report detailing, in respect of any accredited services provided by the accredited entity in a digital ID system other than the Australian Government Digital ID System, the following:
  (a) the number of cyber security incidents that occurred in the reporting period in relation to the entity's accredited services and DI data environment (if any); and
  (b) for each incident:
    (i) the date and time of the incident;
    (ii) a description of the type of incident;
    (iii) the number of digital IDs affected (if any); and
    (iv) the severity of the incident; and
  (c) a description of the measures taken by the entity in response to the incidents covered by the report.

(4) Subject to rule 7.8, a record required by this rule must:
  (a) be retained for a minimum of 3 years from the day it was generated; and
  (b) not contain biometric information.

Subdivision D—Information technology system controls

4.19 Essential Eight

(1) Subject to subrule (2), an accredited entity must, in relation to its DI data environment, implement and comply with all mitigation strategies whose 'relative security effectiveness rating' is marked 'essential' in the document titled *Strategies to Mitigate Cyber Security Incidents* 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.

(2) An accredited entity is not required to comply with a mitigation strategy specified in subrule (1) if the most recent report of an assessor conducting a protective security assessment for the accredited entity includes the assessor's opinion that the strategy 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 or strategy is not relevant to an entity.

Example: A control about Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate, will not be relevant to an entity if the entity does not use Microsoft products within its DI data environment.

4.20 Logging requirements

(1) Any information technology system through which an accredited entity provides 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) any creation, update, use, disclosure or destruction of personal information;
(b) if biometric information is collected or retained by or on behalf of an ISP—the destruction of that biometric information;
(c) successful or failed elevation of access privileges by personnel;
(d) additions, deletions or modifications to personnel or group permissions;
(e) system alerts or failures related to cyber security risks; and
(f) unauthorised attempts to access critical systems or files.

Logging implementation and monitoring plan

(3) An accredited entity must have, maintain and comply with a plan (***logging implementation and monitoring plan***) that details:
(a) how the entity generates, stores, protects, monitors and analyses logs; and
(b) how the entity monitors logs to identify any anomalous behaviour.

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

Note: If an accredited 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.

(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 any entities involved in the event;

(d) any unique identifier used in the event;

(e) the date and time of the event;

(f) for an IXP—each kind of attribute conveyed for the event;

(g) for accredited entities other than an IXP—the types of attributes requested and disclosed to each entity involved in the event; and

(h) if the interaction type 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 any express consent was obtained from the individual;

(ii) the duration of the express consent; and

(iii) whether the express consent was granted or withdrawn by the individual.

(6) A log required by this rule must include, for a kind of entity specified in column 1 of an item in the following table, a record of the matter specified in column 2 of that item.

Logging requirements

Item	Column 1 Kind of entity	Column 2 Matter to be recorded
	Accredited identity service providers	
1	ISP	The binding of attributes to a digital ID.
2	ISP that provides reusable digital IDs	All of the following: (a) the information required to implement and support rate limiting (see the Accreditation Data Standards); (b) the date and time the authenticator was bound to any individual's digital ID; (c) the unique identifier assigned to each individual within the digital ID system in which the entity operates; (d) details of any physical authenticators bound to the digital ID of an individual; and (e) details of the source of any unsuccessful authentications attempted with the authenticator.
3	ISP that conducts biometric binding	Information associated with each biometric binding transaction, including the method of biometric binding used in the transaction.

Logging requirements		
Item	**Column 1** **Kind of entity**	**Column 2** **Matter to be recorded**
4	ISP that conducts manual face comparison activities	All of the following: (a) the manual face comparison activities conducted during the biometric binding process; and (b) the assessing officer responsible for conducting any activities related to the biometric binding transaction.
	Accredited attribute service providers	
5	ASP	All of the following: (a) the retrieval of any special attribute by a third party; (b) the IP Level of the digital ID used to obtain any special attribute from the ASP; and (c) if available, the unique identifier assigned to the digital ID within the digital ID system in which the ASP operates.

(7) Subject to rule 7.8, a log required by paragraphs (2)(a) and (b), subrule (5) and subrule (6) must:
  (a) be retained for a minimum of 3 years from the day it was generated; and
  (b) not contain biometric information.

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 that 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) 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) comply with TLS version 1.2 or higher; and
  (b) follow any 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/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography.

Rule 4.23

4.23 Cryptographic key management processes and procedures

(1) An accredited entity must develop, implement and maintain documented, effective and secure cryptographic key management processes and procedures for its information technology system.

(2) The entity's cryptographic key management processes and procedures must 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 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.

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

Rule 4.25

Division 2—Fraud controls

4.25 Fraud risk assessment

(1) An accredited entity must, for each reporting period, conduct 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 or standard; and
  (b) as part of the fraud risk assessment:
    (i) assess the entity's fraud risks in accordance with the risk matrix developed in accordance with paragraph (a);
    (ii) record the results of the assessment;
    (iii) determine and record the entity's level of tolerance to fraud risks; and
    (iv) record how the entity's controls for fraud risks are applied to its accredited services and DI data environment.

(3) If an ISP collects, uses, holds, discloses or destroys biometric information, the ISP must assess and record in its fraud risk assessment the fraud risks, mitigation strategies and any other actions the ISP will take to address risks related to biometric information.

Applicants

(4) If subrule (1) applies to an applicant because of rule 2.3, the words 'for each reporting period' appearing in that subrule are to be ignored.

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 as 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 (***fraud controller***).

(2) The fraud controller must have responsibility for:
  (a) managing fraud risks; and
  (b) facilitating the entity's compliance with the fraud control requirements specified in this Part.

(3) 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.

(4) 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 that each of 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

An ISP must provide advice to individuals about how to safeguard their digital ID against digital ID fraud risks and update that advice, as soon as practicable, as new risks and threats emerge.

4.30 Support to individuals

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

(2) For the purposes of subrule (1), support services must, at a minimum, include the provision of:

(a) one of the following:

(i) a monitored chat function; or

(ii) a monitored email function; or

(iii) a call centre; and

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

Rule 4.31

Division 3—Fraud control plan

4.31 Fraud control plan

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

(2) An entity of the kind specified in column 1 of an item in the following table must, at a minimum, detail each matter specified in column 2 of that item in the fraud control plan.

Fraud control plan requirements

Item	Column 1 Kind of entity	Column 2 Matter to be detailed
	Risks	
1	Accredited entity	All of the following: (a) any fraud risks, threats and vulnerabilities, including any 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 any fraud risks, threats and vulnerabilities; (c) the strategies and controls the entity uses, or proposes to use, to manage the fraud risks, threats and vulnerabilities identified under 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 the entity uses, or will use, when assessing the severity of a digital ID fraud incident; and (f) the entity's key positions with responsibility for managing fraud risks and the duties of those positions.
	Goals and strategic objectives	
2	Accredited entity	All of the following: (a) the entity's goals and strategic objectives to manage and improve its fraud management capability; and (b) the steps that the entity is taking, or proposes to take, to continuously improve its fraud management capability;
	Personnel and training	
3	Accredited entity	The strategies and controls the entity has used, or will use, to ensure the entity's personnel whose

Fraud control plan requirements		
Item	**Column 1** **Kind of entity**	**Column 2** **Matter to be detailed**
		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	
4	Accredited entity	The strategies and controls the entity has used, or will use, for managing and investigating digital ID fraud incidents and reporting digital ID fraud incidents to the Digital ID Regulator.
	Biometric binding	
5	ISP that collects, holds, uses, discloses and destroys biometric information	Details of the ISP's approach to the use of biometric information for digital ID fraud risk management activities.
6	ISP that conducts manual face comparison	All of the following: (a) details of the procedures the ISP has implemented or will implement to detect any fraudulent activities by assessing officers when those officers are conducting manual face comparison; and (b) a description of each location at which the entity undertakes or will undertake biometric binding.
7	ISP that conducts eIDVT	All of the following: (a) the risks, threats and vulnerabilities specific to the use of eIDVT; and (b) the processes and procedures the ISP uses, or will use, to ensure the destruction of acquired images of processed photo IDs.
8	ISP	The process the ISP has undertaken or will undertake 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.
	In-device biometric capability	
9	ISP that 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) If an accredited entity collects, uses, holds, discloses or destroys biometric information, the entity's fraud control plan must also include details of digital ID fraud risks and associated mitigation strategies and any other actions the entity will take to address risks 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) any capture, temporary storage, and destruction of biometric information;
(d) any biometric matching process the entity implements;
(e) any potential and known threats and attacks to the entity's biometric capability; and
(f) using any manual processes conducted by assessing officers to complete local biometric binding.

4.32 Review of entity's fraud control plan

(1) An accredited entity must review and update its fraud control plan:
(a) at least once in each reporting period; and
(b) as soon as practicable after:
(i) the entity becomes aware of any 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;
(ii) the entity becomes aware of any breach of a requirement specified in its fraud control plan; and
(iii) any change in the entity's organisational structure or control, functions or activities, if that change will, or is reasonably likely to, increase fraud risks to the entity's accredited services or DI data environment.

(2) The entity's review of its fraud control plan must, at a minimum:
(a) have regard to any 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, if necessary, update the goals and strategic objectives in the entity's fraud control plan, including:
(i) recording whether each goal and strategic objective has been met; and
(ii) updating the goals and strategic objectives for the next year.

(3) As soon as practicable after the entity has completed each review of its fraud control plan, the entity must make all necessary amendments to its fraud control plan.

(4) Any changes to the entity's fraud control plan must be approved in writing by the 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 subrule (1), the mechanisms must include an accessible process for personnel, individuals, enforcement bodies and other entities to report digital ID fraud incidents to the accredited entity 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 that:
  (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 any 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 if the entity is authorised to disclose such information.

4.35 Record keeping

(1) 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.

(2) For each reporting period, an accredited entity must prepare a report detailing, in respect of any accredited services provided by the accredited entity in a digital ID system other than the Australian Government Digital ID System, the following:
  (a) the number of digital ID fraud incidents that occurred in the reporting period in relation to the entity's accredited services and DI data environment (if any); and
  (b) for each incident:

(i) the date and time of the incident;
(ii) a description of the type of incident;
(iii) the number of digital IDs affected (if any); and
(iv) the severity of the incident; and

(c) a description of the measures taken by the entity in response to the incidents covered by the report.

(3) Subject to rule 7.8, a record required by this rule must:
(a) be retained for a minimum of 3 years from the day it was generated; and
(b) not contain biometric information.

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 each reporting period.

Rule 4.40

4.40 Providing information about express consent

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

4.41 Duration of express consent

(1) This rule applies if an individual gives an accredited entity express consent for the future collection, use or disclosure of the individual's personal information.

(2) An accredited entity providing public-facing accredited services must provide the individual with a clear and simple process to vary or withdraw any consent given in accordance with subrule (1).

(3) Consent given in accordance with subrule (1) expires at the earliest of the following:
  (a) the end of the period of consent specified by the individual (if any) when the individual gave their consent or at any time afterwards;
  (b) if the individual has varied their consent—the end of the period of consent specified by the individual (if any) when the individual varied their consent;
  (c) the end of the period of consent specified by the accredited entity when the entity collected the individual's consent;
  (d) 12 months after the consent was initially given.

(4) An accredited entity must not rely on consent given in accordance with subrule (1) if that consent has been withdrawn or has expired.

4.42 Data minimisation principle

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

(2) If an accredited entity discloses personal information 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, the accredited entity must ensure that the personal information disclosed is limited to the information that is necessary by:
  (a) ensuring that the accredited entity's information technology system allows the relying party to only select the attributes of the individual that the relying party requires to provide the service, or access to the service, to that individual; and
  (b) ensuring that the accredited entity provides only the selected attributes to the relying party.

4.43 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 prevent, detect, manage and investigate digital ID fraud incidents.

4.44 Privacy awareness training

An accredited entity must ensure that each of its personnel whose duties relate to its accredited services or DI data environment complete privacy awareness training covering the entity's 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.

4.45 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 any 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 any notifications required by law; and

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

(3) For the avoidance of doubt, if an accredited entity uses an enterprise or organisation level data breach response plan, that plan must comply with this rule.

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

4.46 Record keeping

(1) 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.

(2) Subject to rule 7.8, a record required by this rule must:

(a) be retained for a minimum of 3 years from the day it was generated; and

(b) not contain biometric information.

Rule 4.47

Part 4.4—Accredited services must be accessible and inclusive

4.47 Application

This Part applies for the purposes of subsection 30(1) of the Act.

4.48 Reporting on accessibility

Once in each reporting period, an accredited entity must prepare a report detailing:

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

(b) any reasonable steps the entity proposes to take in the next reporting period to 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.

4.49 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 accredited services in a clear and simple manner, using plain language that is easy to understand; and

(c) take reasonable steps to ensure public-facing information related to 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 public-facing information related to accredited services on 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 ensure public-facing accredited services and public-facing information related to accredited services satisfy the Level AA Success Criteria 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 providing public-facing accredited services and public-facing information related to 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 Components 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 1: 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*) of Part 3.3 of Chapter 3, 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 providing 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 monitored chat function, call centre or a telephone support line. Alternative channels may include an in-person shopfront.

(6) An accredited entity providing 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 public-facing accredited services;

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

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

Rule 4.50

Part 4.5—Biometric information: testing and fraud activities

4.50 Requirements if 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 only undertake testing using biometric information for one or more of the following purposes:

(a) to identify whether the thresholds of its technology for presentation attack detection are set correctly, including whether 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) if the testing is unable to be conducted effectively using relevant and representative synthetic or anonymised biometric 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 plan (***testing plan***) that includes the information specified in subrule (4).

(4) A testing plan must include the following information:

(a) the objectives of the testing;

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

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

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

(c) the frequency and duration of the 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 (4)(d), ISO/IEC 24745 outlines how to protect biometric information that is stored.

(5) An accredited entity must ensure that any testing using biometric information 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 using biometric information conducted in that reporting period and containing the following information:

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

(b) the number of transactions that were tested;

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

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

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

(f) in respect of testing conducted for a purpose specified in paragraph (2)(c), (d) or (f)—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 is 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.

4.51 Requirements if biometric information is used for fraud activities

For the purposes of 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 digital ID fraud risk management 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.

Rule 4.52

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

4.52 DI data environment

At least once in each 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 as at the time of the review.

4.53 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) if no such material changes occur—at least once in each reporting period.

Chapter 5—Requirements when providing accredited services

Part 5.1—Accredited identity service providers

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

5.1 General requirements

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

(a) unless 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;

(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 specified as 'must' or 'yes' in the column of the IP Levels Table for the relevant 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 if 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.

5.2 Digital IDs and children

(1) An ISP must not generate a digital ID for an individual who 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 subrule (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.

5.3 One-off digital IDs

(1) An ISP accredited to generate a digital ID that is to be used once only 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 or permitted to retain the attribute in accordance with subrule (2).

(2) For the purpose of subrule (1):
  (a) the ISP may retain the attribute for the purposes of preventing or investigating a digital ID fraud incident for a maximum period of 30 days commencing the day after the attribute is disclosed to the relying party in a transaction; and
  (b) the ISP must retain the attribute if the ISP is required by law (including the Act and these rules) to retain the attribute.

5.4 Use of a reusable digital ID

(1) An ISP must not use a reuseable digital ID of an individual if more than 5 years have elapsed since the digital ID was created.

(2) Subrule (1) does not apply if:
  (a) the digital ID was proofed to IP1 Plus or IP2;
  (b) the ISP verified a document or other credential of the individual listed in Schedules 1 to 4 of these rules within 5 years from the date that the digital ID was created; and
  (c) less than 5 years have elapsed since the ISP last verified a document or other credential of the individual listed in Schedules 1 to 4 of these rules.

(3) Subrule (1) does not apply if:
  (a) the digital ID was proofed to IP2 Plus, IP3 or IP4;
  (b) the ISP conducted biometric binding in respect of the digital ID within 5 years from the date that the digital ID was created; and
  (c) less than 5 years have elapsed since the ISP last conducted biometric binding in respect of the digital ID.

(4) If a reuseable digital ID was created before the commencement of these rules:
  (a) a reference to an ISP in this rule is taken, for the purpose of this rule, to include a reference to that entity at a time before the entity was accredited in accordance with the Act; and
  (b) a reference to an IP level in this rule and in the definition of 'biometric binding' is taken, for the purpose of this rule, to be a reference to an equivalent level of identity proofing.

5.5 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) the step-up is 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.

5.6 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) 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.

5.7 Suspending the use of a digital ID

If an individual requests that an ISP temporarily suspend the use of 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;
  (c) following the suspension, notify the individual of the suspension and the process to resume their digital ID.

Note: See rule 5.9 for resumption of a suspended digital ID.

5.8 Digital IDs affected by a fraud or cyber security incident

(1) If 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 the use of that digital ID.

5.9 Resuming the use of a digital ID

(1) When resuming the use of a digital ID that was temporarily suspended in accordance with rule 5.7, the ISP must ensure:

(a) the individual completes identity proofing at the 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.

(2) When resuming the use of a digital ID that was suspended in accordance with subrule 5.8, the ISP must ensure the individual completes identity proofing at the identity proofing level of the suspended digital ID.

(3) The ISP is not required to resume the use of a digital ID that was suspended if the ISP no longer holds the information that would enable it to do so.

Division 2—Identity proofing and use of credentials

Subdivision A—Identity proofing

5.10 IP Levels Table

(1) The IP Levels Table:
  (a) specifies 6 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) specifies minimum requirements for each identity proofing level.

(2) The requirements in the IP Levels Table do 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 5.1(2)).

Rule 5.10

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 by the ISP to confirm the identity is not known to be used fraudulently	—	Must	Must	Must	Must	Must

IP Levels Table

Item	Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
7	Personnel undertaking identity proofing processes, including visual verification, are provided with tools and training to detect fraudulent attributes, documents or other credentials, before starting work on these duties and annually thereafter	—	Must	Must	Must	Must	Must
8	Documents or other credentials in languages other than English are translated by a National Accreditation Authority for Translators and Interpreters accredited translator	—	—	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 verified using only source verification or technical verification	No	Yes	Yes	Yes	Yes	Yes

Rule 5.10

IP Levels Table

Item	Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
	Credentials required for verification						
10	Verification of a CoI credential must be undertaken			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	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 family names, given names or date of birth 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.

5.11 Verification using an Australian passport

(1) For items 10 and 11 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 the IP Levels Table, 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.

5.12 Technical verification of credentials

If 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 ePassport, if the issuing country publishes a certificate revocation list, review that list to establish whether the foreign ePassport has been cancelled.

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

5.13 Source verification using non-government credentials

If 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.

5.14 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

(b) 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.

Rule 5.15

Subdivision B—Verification using biometric information

5.15 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.

5.16 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) If 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.

5.17 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) for identity proofing at level IP2 Plus only—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/IEC 29794-5 when generating the image quality profile of the acquired image.

(4) An ISP must record evidence of the characteristics used in generating the image quality profile and quality threshold for the acquired image (as required by subrule (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/IEC 30107-1, must be used.

5.18 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 of the following processes:
   (a) technical biometric matching;
   (b) source biometric matching;
   (c) for identity proofing at level IP2 Plus only—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.

Note: For manual face comparison requirements, see rule 5.21.

(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 5.17.

(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.

5.19 Requirements for technical biometric matching

(1) Technical biometric matching of an acquired image must only be conducted using an Australian passport or foreign ePassport if that passport has been technically verified in accordance with rule 5.12.

(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 Australian passport or foreign ePassport.

5.20 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) a driver's licence issued under a law of a State or Territory;
  (b) a proof-of-age card issued by or on behalf of a State or Territory; or
  (c) an 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 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 to have 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 5 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 5.

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

(7) 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.

(8) 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;
(c) the image has passed the quality threshold for the facial image quality profile; and
(d) the ISP must follow the requirements described by ISO/IEC 29794-5 when determining the method to be used for generating the image quality profile of the facial image acquired from the photo ID.

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

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

5.21 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 https://fiswg.org/fiswg_guide_for_facial_comp_awareness_trng_assessors_v1.1_20220617.pdf.

(b) provide assessing officers with a current reference document outlining practicable 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 system 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

5.22 Accessible and inclusive services

This Subdivision:

(a) applies for the purposes of subsection 30(1) of the Act; 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 (***alternative proofing process***).

5.23 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.

(2) An alternative proofing process may include one or more of the following:

(a) acceptance of documents or other credentials not listed in Schedules 1 to 4;

(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;

(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) if an individual lives in a remote area—providing 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.

Example: For paragraph 2(c), Aboriginal and Torres Strait Islander organisations may be able to verify the identity of an individual if no government record for that individual exists.

(3) 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 any 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 details of any controls and risk mitigation strategies to be implemented in response to the identified risks.

(4) For the purpose of this rule, ***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 documents 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.

Division 3—Generating, binding, managing or distributing authenticators

5.24 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 2 of the AL Table for the particular authentication level in column 3, 4 or 5 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) If 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) 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.

(6) 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.

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

(8) 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.

5.25 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.

5.26 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) If 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 may only be a memorised secret or physical authenticator.

5.27 Expired and renewed authenticators

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

(2) As soon as practicable 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 is not allowed to use the authenticator by taking appropriate action considering the authenticator type.

(3) For the purpose of subrule (2), appropriate action may include ensuring the individual has:
(a) surrendered, or proved destruction of, a physical authenticator containing attribute certificates signed by the ISP; or
(b) deactivated the authenticator, uninstalled the authenticator from the device, or had their access to the authenticator revoked.

5.28 Revocation and termination of an authenticator

(1) An ISP must revoke an authenticator, as soon as practicable, if:
(a) an individual's digital ID associated with that authenticator ceases to exist;
(b) an individual requests that the authenticator be revoked; or
(c) the ISP determines that the individual no longer meets its eligibility requirements.

Note: For paragraph (1)(c), this may be because the individual has died or the digital ID is fraudulent.

(2) As soon as practicable after the revocation of an attribute certificate or termination of the individual's authenticator, the ISP must ensure the individual is no longer able to use the authenticator by taking appropriate action considering the authenticator type.

(3) For the purpose of subrule (2), appropriate action may include ensuring the individual has:

(a) surrendered, or proved destruction of, a physical authenticator containing attribute certificates signed by the ISP; or

(b) deactivated the authenticator, uninstalled the authenticator from the device, or had their access to the authenticator revoked.

Rule 5.29

Division 4—Accessibility and useability

5.29 Application

This Division applies for the purposes of section 30 of the Act.

5.30 Verification services

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

(2) An ISP must provide individuals who are undergoing the identity proofing process with a clear and simple description of each step of the 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 accredited services.

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

(4) An ISP must:
(a) provide individuals with information about the documents or other credentials that may be requested to verify the individual's identity at a particular identity proofing level, including information about the combinations of documents or other credentials that will satisfy the request if more than one document or other credential is required;
(b) notify individuals as to whether the provision of 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 the following:
(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 notify an individual of the outcome of the identity proofing process as follows:
(a) if the identity proofing process has been successfully completed—by providing the individual with confirmation of the successful identity proofing and information on the next steps to be taken by the individual (if any);
(b) if the identity proofing process has been partially completed—by providing the individual with details of:
(i) any information, documents or other credentials that will be destroyed by the entity;

(ii) any information, documents or other credentials that will be retained by the entity and the period for which they will be retained; and

(iii) any additional information, documents or other credentials that the individual would need to provide in order to successfully complete the identity proofing process; and

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

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

(ii) clear and simple instructions about how to use any applicable alternative channels or support; and

(iii) the option to either:

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

(B) not continue with the proofing process.

(7) An ISP must notify an individual in accordance with subrule (6) as soon as practicable after the outcome of the identity proofing process is known to the ISP.

(8) If an individual elects:

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

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

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

(ii) notify the individual that the information will be destroyed.

5.31 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) if the ISP issues authenticators that expire, when the authenticator will expire; and

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

Rule 5.32

Part 5.2—Accredited attribute service providers

5.32 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 an 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.

5.33 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 if 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.

5.34 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.

5.35 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 5.3—Accredited identity exchange providers

5.36 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 the participants to that transaction.

5.37 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 or 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 that provides services in the digital ID system that are not accredited services (***unaccredited ISP***);
  (b) allow the IXP or another person to revoke the unaccredited ISP's participation in the digital ID system for non-compliance with the system rules;
  (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) prohibit 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.

Rule 6.1

Chapter 6—Annual reviews

Part 6.1—Accredited entities to conduct annual reviews

6.1 General requirements

(1) Before the end of each period specified in rule 6.2 for an accredited entity (***reporting period***), the accredited entity must conduct a review in accordance with this Part (***annual review***).

(2) The accredited entity must, in respect of each reporting period:
  (a) prepare a report in accordance with Part 6.2 of this Chapter; 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 practicable to the end of the reporting period for that review.

6.2 Reporting periods

Transitioned accredited entities

(1) A transitioned accredited entity may nominate a first annual review date if the entity:
  (a) nominates a first annual review date that is any date after 30 June 2025 and before 1 July 2026; and
  (b) gives the nomination, in writing, to the Digital ID Regulator on or before 30 January 2025.

(2) If a transitioned accredited entity has nominated a first annual review date in accordance with subrule (1), the reporting period for that entity is:
  (a) for the entity's first reporting period—the period beginning on the day the Act commenced and ending on the first annual review date nominated by the entity in accordance with subrule (1); and
  (b) for subsequent reporting periods—each 12-month period after the period mentioned in paragraph (a).

(3) The reporting period for a transitioned accredited entity not covered by subrule (2) is:
  (a) for the entity's first reporting period—the period beginning on the day the Act commenced and ending 12 months after that date; and
  (b) for subsequent reporting periods—each 12-month period after the period mentioned in paragraph (a).

Example: An entity which must complete its first annual review by 1 December 2025 must complete subsequent annual reviews by 1 December of each subsequent year.

Other accredited entities

(4) The reporting period for an accredited entity not covered by subrule (2) or (3) 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; and

(b) for subsequent reporting periods—each 12-month period after the period mentioned in paragraph (a).

6.3 Scope of annual review

Review of changes

(1) An accredited entity must, for each reporting period, identify any changes to the entity's accredited services and DI data environment that may affect the entity's ability to comply with its obligations under the Act, these rules or the Accreditation Data Standards.

(2) The accredited entity must:

(a) for each change identified:

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

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

(iii) assess whether the change is a material change; and

(b) update the entity's statement of scope and applicability to address each material change identified; and

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

Response to material changes

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

(a) conduct an assurance assessment or systems testing to the extent required:

(i) to assess or test the effect of the material change; and

(ii) to ensure and demonstrate that the entity continues to be able to comply with the controls and requirements under the Act, these rules or the Accreditation Data Standards, affected by the material change;

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

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) conduct technical testing to the extent that the material change relates to one of the requirements specified in subrule 2.5(2), to ensure the entity's information technology system continues to have the functionality necessary to meet those requirements, and record in respect of that testing each of the matters specified in subrule 2.5(3); and

(c) if the accredited entity is an ISP that conducts biometric binding or authentication using biometric information—conduct testing of the presentation attack detection technology, the biometric matching algorithm, source biometric matching or the eIDVT in respect of the activities affected by the material change.

(4) 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.

6.4 Assurance assessments

Fraud assessment

(1) An accredited entity must 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 2 years, a fraud assessment has been conducted;
(b) the assessor who conducted the most recent fraud assessment meets the requirements in subrule 3.6(2);
(c) that assessor prepared a report for the most recent fraud assessment in accordance with rule 3.17; and
(d) that assessor stated in their report 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 must conduct a protective security assessment in the reporting period after its first reporting period and thereafter in every alternate reporting period.

6.5 Penetration and presentation attack detection testing

Penetration testing

(1) An accredited entity must cause an assessor to conduct penetration testing, and the entity must provide a report of its response to the assessor's report, in each reporting period.

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

Testing for presentation attack detection

(2) An ISP that conducts online biometric binding or authentication using biometric information using a custom biometric capability must conduct testing for presentation attack detection in the reporting period after its first reporting period and thereafter in every alternate reporting period.

Note: For testing of presentation attack detection technology, see section 2.3 of the Accreditation Data Standards.

Rule 6.6

Part 6.2—Accredited entities to provide annual reports

6.6 Content of annual report

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

6.7 If previous timeframes to address risks and recommendations not met

(1) This rule applies if an accredited entity's response to an assessor's report or a privacy impact assessment:
  (a) provides a timeframe for the entity to take measures to address an identified risk or a recommendation in the report or privacy impact assessment; and
  (b) at the time of the entity's annual review, the entity has failed or is likely to fail to implement the measures in accordance with that timeframe.

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

(3) This rule applies regardless of when the relevant assessor's report or privacy impact assessment was provided to the entity.

6.8 Information and documents

An entity's annual report must include the following information and documents:
  (a) if the entity has updated the boundaries of its DI data environment in accordance with rule 4.52, a copy of the updated documentation;
  (b) if the entity has updated its statement of scope and applicability in accordance with rule 4.53, a copy of the updated statement;
  (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;
  (f) a copy of the accredited entity's fraud risk assessment;
  (g) a copy of the accredited entity's report on accessible services prepared in accordance with rule 4.48;
  (h) a copy of the accredited entity's report on any cyber security incidents prepared in accordance with rule 4.18;
  (i) a copy of the accredited entity's report on any digital ID fraud incidents prepared in accordance with rule 4.35;
  (j) 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 that assessment;
  (k) for an ISP that conducts testing in accordance with paragraph 6.3(3)(c), a copy of those test results; and

(l) for an ISP that conducted testing using biometric information of an individual for testing activities in the reporting period, a copy of the report of that testing prepared in accordance with subrule 4.50(6).

6.9 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 any changes in accordance with rule 6.3 and correctly identified any material changes;

(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) if a cloud service provider conducts 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);

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

(f) the entity has complied with the Act, these rules and the Accreditation Data Standards during the relevant reporting period, with the exception of any non-compliance which the entity has notified to the Digital ID Regulator; and

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

Rule 7.1

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	Collection of the 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	IXP	May collect a restricted attribute of an individual	Collection is for one of the following purposes: (a) providing accredited services to other participants in the digital ID system in which the IXP operates; (b) detecting, reporting or investigating a contravention, or an alleged contravention, of a provision of the Act, these rules or the Accreditation Data Standards; (c) conducting proceedings in relation to a contravention, or an alleged contravention, of a civil penalty provision of the Act; (d) detecting, reporting or investigating a digital ID fraud incident within the digital ID system in which the IXP operates; (e) detecting, reporting or investigating a cyber security incident within the digital ID system in which the IXP operates;

Rule 7.3

Accreditation conditions

Item	Column 1 Entity	Column 2 Condition	Column 3 Circumstances
			(f) conducting an assessment of a matter referred to in paragraph 33C(1)(g) of the Privacy Act; (g) detecting, reporting, investigating or prosecuting an offence against a law of the Commonwealth, a State or a Territory; or (h) if the IXP has engaged a contractor to provide an accredited service, or part of an accredited service, and the following apply: (i) the collection is for the purposes of the contractor providing an accredited service, or part of an accredited service, of the IXP; and (ii) the contractor is contractually bound to comply with the same obligations as apply to the IXP in respect of that information.
3	IXP	May disclose a restricted attribute of an individual	Disclosure is for one of the following purposes: (a) providing accredited services to other participants in the digital ID system in which the IXP operates; (b) detecting, reporting or investigating a contravention, or an alleged contravention, of a provision of the Act, these rules or the Accreditation Data Standards; (c) conducting proceedings in relation to a contravention, or an alleged contravention, of a civil penalty provision of the Act; (d) detecting, reporting or investigating a digital ID fraud incident within the digital ID system in which the IXP operates; (e) detecting, reporting or investigating a cyber security incident within the digital ID system in which the IXP operates; (f) conducting an assessment of a matter referred to in paragraph 33C(1)(g) of the Privacy Act; or (g) detecting, reporting, investigating or prosecuting an offence against a

Rule 7.3

Accreditation conditions

Item	Column 1 Entity	Column 2 Condition	Column 3 Circumstances
			law of the Commonwealth, a State or a Territory.
4	ASP	May collect a restricted attribute of an individual; or may collect a photo of the individual, or biometric information derived from the photo, on a document or other credential provided by the individual	Collection is for the purpose of using that restricted attribute or biometric information to verify a special attribute of the individual.
5	ISP	May collect a restricted attribute of an individual that is on, or derived from, a credential provided by the individual	Collection is for the purpose of providing the ISP's accredited services.
6	ISP	May collect biometric information that is an acquired image provided by the individual; or may collect a photo of the individual, or information derived from the photo, on a document or other credential provided by the individual	Collection is for the purpose of verifying the identity of the individual or authenticating the individual to their digital ID
7	ISP	May disclose a restricted attribute or biometric information to an authoritative source, or to a service that confirms the veracity of an attribute or a document or credential with an authoritative source	Disclosure is for the purpose of verifying the identity of the individual.
8	All accredited entities	May disclose restricted attributes or biometric information to a contractor engaged by the accredited entity to provide an accredited	If: (a) the disclosure is for the purpose of the contractor providing an accredited service, or part of an accredited service, of the accredited entity; and

Rule 7.3

Accreditation conditions

Item	Column 1 Entity	Column 2 Condition	Column 3 Circumstances
		service, or part of an accredited service	(b) the contractor is contractually bound to comply with the same obligations as apply to the accredited entity in respect of that information.

Part 7.3—Reportable incidents

7.4 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;

(b) any matter that could reasonably be considered relevant to whether the entity is a fit and proper person for the purposes of the Act, these rules and the Accreditation Data Standards; or

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

Note: For paragraph (b), 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.

7.5 Change of control for corporations

(1) Subject to subrule (2), this rule applies to:

(a) an accredited entity that is a corporation; and

(b) an entity that is a corporation whose accreditation is suspended;

(2) This rule does not apply to a corporation that is controlled by:

(a) the Commonwealth or an authority of the Commonwealth;

(b) a State or an authority of that State; or

(c) a Territory or an authority of that Territory.

(3) However, this rule applies to a corporation mentioned in subrule (2) if, as a result of a change in control, or a future change in control, the corporation ceases to be, or will cease to be, controlled by:

(a) for a corporation controlled by an entity mentioned in paragraph (2)(a)—an entity mentioned in paragraph (2)(a);

(b) for a corporation controlled by an entity mentioned in paragraph (2)(b)—an entity mentioned in paragraph (2)(b); or

(c) for a corporation controlled by an entity mentioned in paragraph (2)(c)—an entity mentioned in paragraph (2)(c).

(4) The entity must notify the Digital ID Regulator, in accordance with this rule, of a change in control, or a future change in control, of the entity.

(5) The notification must include the following information:

(a) the entity's name;

(b) the contact details for the entity;

(c) the following details in respect of each entity that, through the change or future change in control of the entity, has started or would start to control the entity (***incoming entity***):

(i) the name of the incoming entity;

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

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

(iv) the other contact details of the incoming entity;
(v) if the incoming entity was incorporated outside Australia—the location of its incorporation and the address of its principal place of business in Australia;
(vi) the business name or names of the incoming entity;
(vii) the date on which the incoming entity was registered under the Corporations Act or other law;
(viii) the names and director identification number of each of the directors and other officers of the incoming entity;
(ix) in respect of each subsidiary of the incoming entity—the information specified in subparagraphs (i) to (viii); and

(d) the date on which the change of control occurred or is expected to occur.

(6) The notification must be made:
(a) if the entity becomes aware that, at any time in the future, a change in control of the entity will occur—within 72 hours after the entity becomes aware; or
(b) otherwise—within 72 hours after the change in control occurs.

(7) Without limiting paragraph (6)(a), an entity is taken to be aware that a change in control of the entity will occur at the time:
(a) a resolution is passed by the entity regarding the change in control; or
(b) a court order regarding the change in control is made.

(8) In this rule:

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

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

Commonwealth company has the meaning given in the *Public Governance, Performance and Accountability Act 2013.*

control:
(a) in relation to a ***Commonwealth company***—has the meaning given in section 89 of the *Public Governance, Performance and Accountability Act 2013*;
(b) otherwise—has the meaning given in section 910B of the Corporations Act.

corporation has the meaning given in the Corporations Act.

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

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

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

7.6 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 intention and details of its plans, as soon as practicable after forming that intent.

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

Rule 7.7

Part 7.4—Data standards relating to accreditation

7.7 Digital ID Data Standards Chair to make standards

(1) For the purposes of 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, for the matters specified in subrule (2).

(2) The matters are:

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

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

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

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

(e) test standards for an entity's information technology system utilising 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 5.1(1)(a)(ii)).

Part 7.5—Record keeping

7.8 General record keeping requirement

An 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 is not biometric information; and

(c) the information was obtained by the entity in the course of providing accredited services; and

(d) 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

(e) the information relates to:

(i) any current or anticipated legal proceedings; or

(ii) any dispute resolution proceedings; or

(iii) a current compliance or enforcement investigation under 'this Act' (as defined in section 9 of the Act);

to which the entity is a party.

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 5.1(1)(a)(iii) (requirement for verification of a document or other credential).

Item	Column 1 Document or other credential used for verification:	Column 2 Must be verified by:
1	Birth certificate issued by a State or Territory government	Source verification.
2	Australian passport that is current or, if expired, no more than 3 years past the expiry date	Source verification or technical verification
3	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.
4	Australian Certificate of Registration by Descent issued by the Australian Government	Source verification.
5	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.
6	Certificate of Identity document issued by the Department of Foreign Affairs and Trade	Source verification.
7	Australian Document of Identity issued by the Department of Foreign Affairs and Trade	Source verification.
8	Convention Travel Document, also known as a *Titre de Voyage* issued by the Department of Foreign Affairs and Trade	Source verification.
9	ImmiCard issued to an individual 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 5.1(1)(a)(iii) (requirement for verification of a document or other credential).

Item	Column 1 Document or other credential used for verification:	Column 2 Must be verified by:
1	Marriage certificate issued by or on behalf of a State or Territory	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*	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 5.1(1)(a)(iii) (requirement for verification of a document or other credential).

Item	Column 1 Credential used for verification:	Column 2 must be verified by:
1	Concession or health care card issued by Services Australia	Source verification.
2	Medicare card (as defined by section 84 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 (as defined by section 3 of the *National Vocational Education and Training Regulator Act 2011*)	Source verification or visual verification.
4	Debit or credit card that is current and issued by an authorised deposit-taking institution (as defined by section 5 of the *Banking Act 1959*)	Source verification.
5	Veteran Card issued by the Department of Veterans' Affairs	Source verification or visual verification.
6	Document evidencing an individual's enrolment on the electoral roll maintained by the Australian Electoral Commission	Source verification.
7	Photo ID—a document or other credential listed in Schedule 4, but only if that document or other credential has not already been used for the purposes of satisfying a particular requirement of an IP level of the IP Levels Table	The verification requirements for that document or other credential specified in Schedule 4.

Schedule 4—Documents or other credentials that are a photo ID

Note: See rule 1.4 (definition of 'photo ID') and subparagraph 5.1(1)(a)(iii) (requirement for verification of a document or other credential).

Item	Column 1 **Documents or other credentials that contain a photo of the individual:**	Column 2 **Must be verified by:**
1	Australian passport that is current or, if expired, no more than 3 years past the expiry date	Source verification or technical verification.
2	Driver's licence issued under the law of a State or Territory	Source verification.
3	Foreign passport, other than an ePassport, issued by the government of a foreign country	Visual verification.
4	Foreign ePassport issued by the government of a foreign country	Technical verification.
5	Convention Travel Document, also known as a *Titre de Voyage*, issued by the Department of Foreign Affairs and Trade	Source verification.
6	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.
7	Shooter or firearms licence issued under a law of a State or Territory	Source verification or visual verification.
8	Identity card issued under section 78 of the *Aviation Transport Security Act 2004* or section 137 of the *Maritime Transport and Offshore Facilities Security Act 2003*	Source verification.
9	Proof-of-age card issued by or on behalf of a State or Territory	Source verification or visual verification.
10	Working with children or vulnerable people card issued by or on behalf of a State or Territory	Source verification or visual verification.
11	ImmiCard issued to an individual 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 5—PSPF controls

Note: See rule 4.3 (compliance with the PSPF).

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
1	PSPF Policy 1	B.1		The accountable authority of each entity must:	(a) determine their entity's tolerance for security risks
2	PSPF Policy 1	B.1		The accountable authority of each entity must:	(b) manage the security risks of their entity, and
3	PSPF Policy 1	B.1		The accountable authority of each entity must:	(c) consider the implications their risk management decisions have for other entities, and share information on risks as appropriate.
4	PSPF Policy 2	B.1		The accountable authority must:	(a) appoint a Chief Security Officer (***CSO***) at the Senior Executive Service level to be responsible for security in the entity
5	PSPF Policy 2	B.1		The accountable authority must:	(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

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
					(iv) investigating, responding to, and reporting on security incidents, and
6	PSPF Policy 2	B.1		The accountable authority must:	(e) 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.
7	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 and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.	
8	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
9	PSPF Policy 2		Requirement 2. Security procedures	Entities must develop and use procedures that ensure:	(b) security incidents are investigated, responded to, and reported, and
10	PSPF Policy 2		Requirement 2. Security procedures	Entities must develop and use procedures that ensure:	(c) relevant security policy or legislative obligations are met.

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
11	PSPF Policy 2		Requirement 3. Security training	Entities must provide all personnel, including contractors, with security awareness training at engagement and annually thereafter.	
12	PSPF Policy 2		Requirement 4. Specific training	Entities must provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training targeted to the scope and nature of the position.	
13	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, cyber and physical security. Note: See the guidance advice in section C.10.4 of PSPF Policy 2 to assist in implementation of this requirement.	
14	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.	
15	PSPF Policy 3	B.1		The security plan must detail the:	(a) security goals and strategic objectives of the entity, including how security risk management intersects with and supports

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
					broader business objectives and priorities
16	PSPF Policy 3	B.1		The security plan must detail the:	(b) threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets
17	PSPF Policy 3	B.1		The security plan must detail the:	(c) entity's tolerance to security risks
18	PSPF Policy 3	B.1		The security plan must detail the:	(d) maturity of the entity's capability to manage security risks, and
19	PSPF Policy 3	B.1		The security plan must detail the:	(e) entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.
20	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.	
21	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.	
22	PSPF Policy 3		Requirement 5. Threat levels	The security plan (and supporting security plans) must include scalable	

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
				measures to meet variations in threat levels and accommodate changes in the National Terrorism Threat Level.	
23	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.	
24	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.	
25	PSPF Policy 4		Requirement 1. Security maturity records	Entities must document and evidence their assessment of the entity's security maturity.	
26	PSPF Policy 6	B.1		Each entity is accountable for the security risks arising from procuring goods and services, and must ensure contracted providers comply with relevant PSPF requirements.	
27	PSPF Policy 6		Requirement 1. Assessing and managing security	When procuring goods or services, entities must put in place proportionate	(a) specific security risks to its people, information and assets, and

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
			risks of procurement	protective security measures by identifying and documenting:	
28	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:	(b) mitigations for identified risks.
29	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
30	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:	(b) manage identified security risks relevant to the procurement, and
31	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:	(c) implement governance arrangements to manage ongoing protective security requirements, including to notify the entity of any actual or suspected security incidents and follow reasonable direction from the entity arising from incident investigations.

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
32	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
33	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:	(b) manage any changes to the provision of goods or services, and reassess security risks.
34	PSPF Policy 6		Requirement 4. Completion or termination of a contract	Entities must implement appropriate security arrangements at completion or termination of a contract.	
35	PSPF Policy 8	B.1		Each entity must:	(a) identify information holdings
36	PSPF Policy 8	B.1		Each entity must:	(b) assess the sensitivity and security classification of information holdings, and
37	PSPF Policy 8	B.1		Each entity must:	(c) implement operational controls for these information holdings proportional to their value, importance and sensitivity.
38	PSPF Policy 8		Requirement 7. Minimum protections and	Entities must ensure information is transferred and transmitted by means that deter and detect compromise and	

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
			handling requirements	that meet the minimum protection requirements set out in Annexes A to C.	
39	PSPF Policy 8		Requirement 8. 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 C. This includes ensuring security classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.	
40	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
41	PSPF Policy 9	B.1		Each entity must enable appropriate access to official information. This includes:	(b) ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information, and
42	PSPF Policy 9	B.1		Each entity must enable appropriate access to official information. This includes:	(c) controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.
43	PSPF Policy 9		Requirement 5. Managing access	To manage access to information systems holding sensitive or security	

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
			to information systems	classified information, entities must implement unique individual identification, authentication and authorisation practices on each occasion where system access is granted.	
44	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 delivery of government business by applying the ISM's cyber security principles during all stages of the lifecycle of each system.	
45	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.	
46	PSPF Policy 11		Requirement 1. Authorisation of ICT systems to operate	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 6	

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
				step risk-based approach for cyber security.	
47	PSPF Policy 11		Requirement 5. Vulnerability Disclosure Program	Entities must have in place a vulnerability disclosure program.	
48	PSPF Policy 12	B.1		Each entity must ensure the eligibility and suitability of its personnel who have access to Australian Government resources (people, information and assets).	
49	PSPF Policy 12		Requirement 1. Pre-employment screening	Entities must undertake pre-employment screening, including:	(a) verifying a person's identity using the DVS (within the meaning of that term in section 15 of the *Identity Verification Services Act 2023*), and
50	PSPF Policy 12		Requirement 1. Pre-employment screening		(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.
51	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.	

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
52	PSPF Policy 14	B.1		Each entity must ensure that separating personnel:	(a) have their access to Australian Government resources withdrawn, and
53	PSPF Policy 14	B.1		Each entity must ensure that separating personnel:	(b) are informed of any ongoing security obligations.
54	PSPF Policy 14		Requirement 1. Sharing security relevant information, debriefs and continuing obligations	Prior to personnel separation or transfer, entities must:	(a) notify the CSO, or relevant security advisor, of any proposed cessation of employment resulting from misconduct or other adverse reasons
55	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
56	PSPF Policy 14		Requirement 2. Withdrawal of access	On separation or transfer, entities must remove personnel's access to Australian Government resources, including:	(b) ICT systems.
57	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.	

Item	Column 1 PSPF Policy	Column 2 B.1 Core requirement	Column 3 B.2 Supporting requirement	Column 4 Requirement	Column 5 Sub-requirement
58	PSPF Policy 15	B.1		Each entity must implement physical security measures that minimise or remove the risk of:	(a) harm to people, and
59	PSPF Policy 15	B.1		Each entity must implement physical security measures that minimise or remove the risk of:	(b) information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
60	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.	
61	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.	
62	PSPF Policy 15		Requirement 3. Disposal	Entities must dispose of physical assets securely.	