Digital ID Accreditation Rules 2024

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

Dated

Katy Gallagher
DRAFT ONLY—NOT FOR SIGNATURE
Minister for Finance

Contents

Chapter 1 Preliminary

1.1 Name

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

1.2 Commencement

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

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
The whole of this instrument	The time at which the *Digital ID Act 2023* commences.	

Note: This table relates only to the provisions of this instrument as originally made.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

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

1.3 Authority

These rules are made under section 158 of the *Digital ID Act 2023* and for the purposes of the provisions in the Act which the term 'Accreditation Rules' occurs.

Note: Each rule is made for the purposes of section 27 of the Act unless otherwise stated in the rule.

1.4 Definitions

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

- accredited entity
- accreditation conditions
- accredited attribute service provider
- accredited identity exchange provider
- accredited identity service provider
- accredited services
- attribute
- attribute service provider
- Australia
- Australian Government Digital ID System
- biometric information
- cyber security incident
- digital ID
- digital ID fraud incident
- Digital ID Regulator
- digital ID system

- enforcement body
- entity
- identity exchange provider
- identity service provider
- participating relying party
- personal information
- privacy impact assessment
- relying party
- restricted attribute

(1) In these rules:

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

ACSC means the Australian Cyber Security Centre.

Act means the *Digital ID Act 2023*.

accreditation day means the day the entity's accreditation comes into force.

annual review means a review required, in accordance with Chapter 6, after an accredited entity's accreditation day.

approved cryptography means:

(a) Australian Signals Directorate Approved Cryptographic Algorithms; and

(b) Australian Signals Directorate Approved Cryptographic Protocols;

as defined in the ISM.

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

assessor—see subrule 3.2(1).

assessor's report—see rule 3.16.

assurance assessment means a protective security assessment, fraud assessment or usability and accessibility assessment—see Part 2 of Chapter 3.

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

Note: See item 4 of Table 1 in rule 5.13

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

biometric matching means one-to-one comparison of an individual against the image on their photo ID using either technical biometric matching, source biometric matching, eIDVT biometric matching or manual face comparison processes.

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

COI credential means a credential that:

(a) evidences the commencement of identity for an individual in Australia; and

(b) is listed in and complies with the requirements of Table 1 of Schedule 1.

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

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

cyber security risk assessment—see rule 4.5.

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

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

digital ID information means information that is:

(a) generated for purposes of or in the provision of an accredited service; or

(b) collected, held, used or disclosed as part of providing or receiving an accredited service.

eIDVT means electronic identity document verification technology that uses non-cryptographic techniques to classify physical credentials as being genuine or not genuine, when submitted online and in real-time by an individual.

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 the photo captured of the individual.

ePassport means a TD3 size Machine Readable Travel Document conforming to the specifications of Part 4 of the ICAO Doc 9303 Standard that additionally incorporates a contactless integrated circuit including the capability of biometric identification of the individual.

fraud assessment—see rule 3.7

fraud management capability—see rule 4.22.

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

fraud risk assessment—see rule 4.23.

held has the same meaning as in the Privacy Act.

ICAO Doc 9303 Standard means the International Civil Aviation Organisation Doc Machine Readable Travel Documents standard.

Note 1: At the commencement of these rules, located at https://www.icao.int/publications/pages/publication.aspx?docnum=9303.

Note 2: See rule 1.5(2) for the time at which an entity must comply with a change to an incorporated instrument for purposes of these rules.

identity proofing means the service if and identity service provider that generates, manages, maintains or verifies information relating to the identity of an individual.

identity proofing level means the level of assurance or confidence in the identity proofing process.

Note: See Table 1 of rule 5.13 for the identity proofing levels applicable to these rules.

IP level means identity proofing level.

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

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

linking credential means a credential that:

(a) demonstrates the continuity of the individual's verified identity where that individual's attributes have changed; and

(b) is listed in and complies with the requirements Table 2 of Schedule 1.

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

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

personnel, of an entity, means:

(a) an employee of the entity; or

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

photo ID means a credential that includes an image of the individual and is listed in, and meeting the requirements of, Table 4 of Schedule 1.

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

presentation attack detection means the detection of a subversive and fraudulent presentation attack at the point of collection of the relevant biometric information.

Privacy Act means the *Privacy Act 1988* (Cth).

protective security assessment—see rule 3.4.

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

Note: At the commencement of these rules, located at https://www.protectivesecurity.gov.au/

public-facing accredited services—see rule 4.45.

public-facing information—see rule 4.45.

reusable digital ID means a digital ID generated, managed, maintained or 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 an authoritative source to verify that an acquired image biometrically matches the corresponding image recorded against that individual's identity at the authoritative source—see rule 5.23.

statement of scope and applicability means a statement, relevant to the accredited services the applicant seeks to provide, and which identifies how the requirements in these rules are applied to, and will be assessed against, the applicant's or accredited entity's DI data environment.

systems testing means penetration testing, usability testing or WCAG testing, each as referred to in Part 3 of Chapter 3.

taking reasonable steps—see subrule 1.61.6(1).

technical biometric matching means biometric matching that meets the requirements of rule 5.22.

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

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

UitC credential means a credential that evidences use in the Australian community of an individual's identity operating and which is listed in and complies with the requirements in Table 3 in Schedule 1.

usability and accessibility assessment—see rule 3.12.

visual verification means the act of a trained member of personnel of an accredited entity visually the physically presented credential is legitimate.

WCAG means the Web Content Accessibility Guidelines published by the Web Accessibility Initiative**.**

Note: At commencement of these rules, located at https://www.w3.org/TR/WCAG21/

1.5 Incorporated instruments

(1) If a provision of these rules incorporates or applies, with or without modification, matters contained in any other instrument or other writing (***incorporated instrument***),

then, unless the contrary intention appears in the provision, the reference to the incorporated instrument is a reference to the incorporated instrument as in force or existing from time to time.

(2) For the purposes of these rules, an accredited entity will not be required to comply with a change to an incorporated instrument until 12 months after the change has been effected in the incorporated instrument.

Note: See paragraph 157(3) of the Act.

1.6 Taking reasonable steps

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

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

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

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

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

(ii) ways of eliminating or minimising the risks;

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

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

Chapter 2 Applying for accreditation

2.1 Criteria to be met

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

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

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

(3) The applicant must have conducted:

(a) each kind of assurance assessment;

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

(c) any other testing as required by these rules.

Note: See Chapter 3 for assurance assessments and systems testing.

2.2 Information and documents to accompany an application

(1) For the purposes of paragraph 135(1)(c) of the Act, an application for accreditation must be accompanied by the following information and documents:

(a) description of the services the applicant would provide as the kind of accredited entity it is applying to be accredited as;

(b) description of any conditions the applicant seeks to be imposed on its accreditation and any documents to support the imposition of the condition;

(c) description of the boundaries of the DI data environment through which the applicant would provide its accredited services;

(d) a statement of scope and applicability;

(e) a copy of each of the assessor's reports and applicant's report responding to the assessor's report required to be prepared for each kind of assurance assessment specified in Chapter 3;

(f) a copy of each of the assessor's reports and applicant's report responding to the assessor's report required to be prepared for each kind of systems testing specified in Chapter 3 where that kind of systems testing applies to the applicant;

(g) a copy of a fraud risk assessment in accordance with rule 4.23;

(h) a copy of a cyber security risk assessment in accordance with rule 4.5;

(i) a copy of the privacy management plan that will be the applicant's plan if accredited;

(j) a copy of a privacy impact assessment conducted in respect of the applicant's DI data environment and proposed accredited services and the applicant's response to that assessment in accordance with rule 2.3;

(k) a copy of the applicant's privacy policy that will be the applicant's policy for the purposes of rule 4.36 if the applicant is accredited;

(l) a copy of the data breach response plan that will be the applicant's plan for the purposes of rule 4.41 if the applicant is accredited;

(m) if the applicant is seeking an accreditation condition to be imposed which authorises the applicant to collect biometric information of an individual, the following documents:

(i) testing plan and processes as required by rule 4.43; and

(ii) the ethical policies and procedures as required by rule 4.44; and

(n) where the applicant intends to provide biometric binding or biometric authentication, the following documents to the extent those documents are relevant to the kind of biometric binding or biometric authentication proposed to be provided by the applicant:

(i) the evaluation results and report for the presentation attack detection technology as required by rule 5.28;

(ii) the evaluation results and report for the biometric matching algorithm in accordance with rule 5.29;

(iii) a copy of evidence of source biometric matching testing as required by rule 5.30; and

(iv) a copy of the evaluation results and the report for the eIDVT testing as required by rules 5.31 and 5.32.

Note 1: For subrule (b), the Act prohibits some conduct unless the conduct is authorised by an accreditation condition —for example, disclosure of restricted attributes and collection and disclosure of biometric information of an individual.

Note 2: The Digital ID Regulator may approve the form and manner of an application. The form may require information and documents to accompany the application (see paragraphs 135(1)(a)-(b) of the Act.

Note 3: The Digital ID Regulator may require an applicant to give further information or documents (see subsection 136(2)) of the Act and is not required to make a decision on the application until the information or documents are given (see subsection 137(3) of the Act).

2.3 Privacy impact assessment

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

(2) The privacy impact assessment must:

(a) be assessed for:

(i) the applicant's DI data environment as the boundaries of that environment are defined in the applicant's application for accreditation; and

(ii) the applicant's proposed accredited services;

(b) be conducted by a person who:

(i) who 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 DI data environment or accredited services; and

(c) include:

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

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

(iii) an analysis of how the applicant's provision of its proposed accredited services will impact the privacy of individuals and protection of personal information;

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

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

(vi) details of consultation with relevant stakeholders.

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

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

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

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

(b) conduct a risk assessment;

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

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

(e) respond to each recommendation in the assessment.

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

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

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

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

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

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

(i) the reasons for the non-acceptance;

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

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

2.4 Technical testing

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

(a) rule 4.14 (incident investigation, management and response - cyber security incidents);

(b) rule 4.18 (logging requirements);

(c) rule 4.31 (incident monitoring and detection - fraud incidents);

(d) rule 4.9 (support to individuals); and

(e) the rules in Chapter 5 that are specific to the kind of accredited entity that the applicant is applying to be accredited as.

(2) 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) a requirements traceability matrix which maps the technical testing completed to each requirement referred to in subrule (1) which is required to be been tested; and

(e) the results of the technical testing, including any defects identified and a description of how such defects have been addressed.

(3) The applicant must include with its application an attestation statement signed by the applicant's accountable executive that the technical testing has been conducted and the applicant is satisfied that the technical testing demonstrates that the requirements tested will be met.

Note: For the purposes of subrule 6.2(3)(b), the references to 'applicant' in this rule 2.4 are taken to mean 'accredited entity'.

2.5 Matters to which the Digital ID Regulator must have regard

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

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

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

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

2.6 DI data environment

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

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

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

(ii) infrastructure owned by, and management provided by, an outsourced service provider or third party;

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

(i) segregation of the environment from other systems;

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

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

(iv) minimising the use of third-party service providers interacting with information referred to in subparagraph (a)(i).

2.7 Compliance with Act and the rules

Unless paragraph 15(4)(b) of the Act applies (where the Digital ID Regulator makes a requirement for a compliance assessment to be conducted)—the Digital ID Regulator must be satisfied that the information and documents provided by the applicant demonstrate that the applicant will be able to comply with the Act and these rules if accredited.

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

Chapter 3 Assurance assessments and systems testing

Part 1—General

3.1 Entity's obligation

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

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

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

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

(a) having regard to the applicant's statement of scope and applicability; and

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

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

3.2 Assessors

(1) The assurance assessments and systems testing must be conducted by an individual:

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

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

(2) If required by the assessor, an entity must take reasonable steps to permit the assessor secure online access to documentation and information related to the assurance assessment or systems testing and to undertake a site visit to the entity's premises or other location at which the accredited services are, or will be, provided.

Part 2—Assurance assessments

Division 1— Protective security assessment

3.3 Interpretation

(1) In this Division:

essential strategies review — see rule 3.5.

3.4 Requirements

(1) A protective security assessment must:

(a) review and assess the entity's implementation and compliance with:

(i) if the entity has chosen to comply with ISO 27001 and 27002, that framework; or

(ii) if the entity has chosen to comply with the PSPF, that framework; or

(iii) if the entity has chosen to comply with another standard or framework, that standard or framework;

(b) review and assess an entity's protective security capability referred to in rule 4.1

(c) review and assess an entity's compliance with the additional protective security controls in rules 4.5 to 4.21;

(d) review and address findings and any recommendations in the penetration testing report referred to in rule 3.11;

(e) review and address findings and any recommendations in the entity's essential strategies review report referred to in subrule 3.5(4); and

(f) if rule 3.6 applies to the entity, comply with the requirements in that rule.

Note: For standards and frameworks in subparagraph (1)(a), see subrule 4.2(1).

(2) For a protective security assessment involving ISO 27001 and 27002, the assessor conducting the assessment must:

(a) be accredited by the Joint Accreditation System of Australia and New Zealand (JASANZ) to certify entities against ISO 27001 and ISO 27002; or

(b) be accredited by an entity recognised by JASANZ to be able to be certify entities against ISO 27001 and ISO 27002; and

(c) meet the following additional requirements:

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

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

(3) For a protective security assessment involving PSPF controls or another standard or framework, the assessor conducting the assessment must meet the following additional requirements:

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

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

3.5 Essential strategies review and report

(1) In this rule:

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

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

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

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

(2) An entity must:

(a) review and assess its compliance with rule 4.17 (***essential strategies review***) by conducting an assessment of its implementation and compliance with the Essential Eight Maturity Model to ISM mapping document for Information Security Manual controls marked maturity level 2; and

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

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

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

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

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

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

3.6 Where a control may not apply

(1) If an entity considers that it cannot comply with a protective security control because of the particular circumstances of the entity or the entity's DI data environment, the entity must:

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

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

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

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

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

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

(iv) whether the assessor considers that the protective security control does not apply to the entity.

Note: For example, an entity may not be able to comply with a control involving physical security because the entity's personnel work remotely and the entity does not have a physical office.

Division 2— Fraud assessment

3.7 Requirement

(1) A fraud assessment must review and assess:

(a) an entity's implementation and compliance with the fraud control requirements in Part 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) The assessor conducting the assessment must meet the following additional requirements:

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

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

Division 3—Usability and accessibility assessment

3.8 Requirements

(1) A usability and accessibility assessment must review and assess:

(a) the entity's implementation and compliance with the usability and accessibility requirements in Part 4 of Chapter 4;

(b) for an accredited identity service provider:

(i) the entity's implementation and compliance with the user experience requirements in rule 5.33;

(ii) if the identity service provider does, or will, provide reusable digital IDs—the entity's compliance with the user experience requirements specified in rule 5.52; and

(c) the findings of any risks and recommendations identified by the WCAG testing required by rule 3.15; and

(d) where the entity is required to conduct usability testing, the findings, risks and recommendations from any usability testing conducted as required by rules 3.12 and 3.13.

Part 3—Systems testing

Division 1—Penetration testing

3.9 Penetration testing requirements

(1) An entity must conduct penetration testing of its DI data environment to evaluate the effectiveness of its security controls by emulating the tools and techniques of likely attackers to exploit security weaknesses.

(2) The penetration testing must be conducted before the protective security assessment referred to in rules 3.3 to 3.6.

3.10 Penetration testing assessor

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

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

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

3.11 Penetration testing report

(1) The assessor must prepare a testing report that includes:

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

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

(c) the test results, including:

(i) any findings and recommendations; and

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

Division 2—Usability testing

3.12 Usability testing requirements

(1) An entity with public-facing accredited services must conduct usability testing of its public-facing DI data environment to:

(a) identify issues in the design and usability of the entity's public-facing DI data environment for users or expected users of its accredited services; and

(b) recommend improvements (if any) to the entity's public-facing DI data environment to:

(i) address any adverse issues to useability and accessibility by individuals identified by the assessment; and

(ii) reduce or mitigate usability issues.

(2) The usability testing must:

(a) involve a diverse range of individuals including individuals with disability, and individuals with a diverse range of age, gender, ability and ethnicity; and

(b) take place across a wide range of devices and platforms so that the testing demonstrates a continuity of support for access to the accredited services across those devices and platforms.

3.13 Usability testing report

(1) The assessor must prepare a testing report that includes:

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

(b) a description of the scope of testing to cover:

(i) findings and quantitative metrics; and

(ii) identification of user issues and recommendations to address accessibility and usability involving the entity's DI data environment.

Division 3—WCAG testing

3.14 WCAG testing requirements

(1) An entity must test whether its public-facing accredited services and public-facing information related to its accredited service meets WCAG version 2.1 to the AA standard (see rule 4.47(2)).

3.15 WCAG testing report

(1) The assessor must prepare a WCAG testing report that includes:

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

(b) the testing results, including:

(i) any findings and recommendations; and

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

Part 4—Reports

3.16 Assessor's report

(1) For each kind of assurance assessment, the assessor must prepare a report (***assessor's report)*** for that assessment that includes, at a minimum:

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

(b) the dates on which the assurance assessment 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 (as relevant);

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

(f) the evaluation or test methodology used in the assurance assessment ; and

(g) the findings of the assurance assessment, including:

(i) details of any non-compliance with the Act and these rules relevant to the assurance assessment;

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

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

3.17 Entity's response to a report of an assessor

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

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

(3) For each risk and recommendation identified in an assessor's report or systems testing report, the 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 its risk matrix;

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

(e) respond to each recommendation in the report.

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

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

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

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

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

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

(i) the reasons for the non-acceptance;

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

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

Chapter 4 Maintaining accreditation

Part 1—Protective security controls

Division 1—Capability

4.1 Protective security capability

(1) ***Protective security capability*** of an accredited entity means the accredited entity's ability to manage protective security of its DI data environment in practice through the implementation and operation of processes and controls, including by:

(a) allocating adequate budget and resources; and

(b) providing for management oversight.

(2) An accredited entity's protective security capability must be appropriate and adapted to respond to cyber security risks, including emerging risks, having regard to:

(i) the extent and nature of the digital ID information that the entity holds;

(ii) the extent and nature of cyber security risks, threats and vulnerabilities;

(iii) the potential loss or damage to one or more individuals if a cyber security incident occurs;

(iv) the potential loss or damage to relying parties if a cyber security incident occurs; and

(v) the potential loss or damage to entities and individuals if a cyber security incident occurs that results in a digital ID being compromised or rendered unreliable.

(3) An accredited entity must take reasonable steps to prevent, detect and deal with cyber security incidents, including by:

(a) having and maintaining a protective security capability;

(b) continuously improving its protective security capability; and

(c) identifying, treating and managing cyber security risks.

Division 2 – Protective security frameworks

4.2 Applicable framework

(1) Subject to subrule (4), an accredited entity must implement, manage, monitor and comply with:

(a) all controls in ISO/IEC 27001 and ISO/IEC 27002; or

(b) the PSPF controls set out at Schedule 2; or

(c) an alternative standard or framework which covers all:

(i) the controls in ISO/IEC 27001 and ISO/IEC 27002; or

(ii) the PSPF controls set out at Schedule 2.

(2) An accredited entity must ensure that the relevant framework in subrule (1)is documented separately, and therefore can be assessed distinctly against, the accredited entity's DI data environment and accredited services.

(3) If an accredited entity chooses to apply controls in an alternative standard or framework referred to in subrule (1)(c), the entity must map those controls against:

(a) the controls in ISO/IEC 27001 and ISO/IEC 27002; or

(b) the PSPF controls set out at Schedule 2,

so as to demonstrate that all control requirements have been met.

(4) An accredited entity is not required to comply with a protective security control in a standard or framework if the most recent report of the assessor conducting a protective security assessment includes the assessor's opinion that the protective security control cannot be complied with by the entity.

Note: See rule 3.6(1)(c)(iv) about controls that cannot be implemented.

4.3 Terms in ISO/IEC 27001 and ISO/IEC 27002

(1) For the purposes of these rules, references to the following terms in ISO/IEC 27001 and ISO/IEC 27002 have the corresponding meaning below:

(a) 'Personally Identifiable Information'—the corresponding meaning is 'personal information'.

(b) 'information security incident'—the corresponding meaning is 'cyber security incident'.

(c) 'information security risk'—the corresponding meaning is 'cyber security risk'.

(2) An accredited entity that elects to implement ISO/IEC 27001 and ISO/IEC 27002 in accordance with subrule 4.2(1)(a):

(a) may implement, manage, monitor and comply with ISO/IEC 27001: 2013 and ISO/IEC 27002: 2013 until 31 December 2024; and

(b) must implement, manage, monitor and comply with ISO/IEC 27001: 2022 and ISO/IEC 27002: 2022 from 1 January 2025.

4.4 Terms in PSPF

(1) For the purposes of these rules, references to the following terms in in the PSPF have the corresponding meaning below:

(a) 'sensitive information'—the corresponding meaning is 'personal information'.

(b) 'Australian Government resources'—the corresponding meaning is 'DI data environment'.

(c) 'risks'—the corresponding meaning is 'cyber security risks'.

Division 3—Additional protective security controls

4.5 Cyber security risk assessment

(1) An accredited entity must at least once in every 12-month period after its accreditation day, conduct an assessment of the cyber security risks associated with its accredited services and DI data environment (***cyber security risk assessment***).

(2) An accredited entity must:

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

(b) for the cyber security risk assessment:

(i) assess the entity's cyber security risks in accordance with the entity's risk matrix;

(ii) record the results of the assessment;

(iii) determine and record the entity's level of tolerance to cyber security risks; and

(iv) record the entity's controls for cyber security risks.

(3) Where an accredited entity collects, uses, holds, discloses or destroys biometric information, the accredited entity must assess cyber security risks (including the risks outlined in rule 4.10(5)), mitigation strategies and treatments related to that biometric information and those processes.

4.6 Sharing information about risks

(1) An accredited entity must:

(a) consider the implications that the entity's decisions related to the management of cyber security risks have for other for other participants of the digital ID system in which the accredited entity operates; and

(b) share information on known cyber security risks or cyber security incidents with those participants where appropriate.

4.7 Eligibility and suitability of personnel

(1) 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 elects to implement the PSPF referred to in rule 4.2(1)(b), this rule 4.7 may be met by the entity complying with the requirements in PSPF Policy 13.

4.8 Advice to individuals

(1) An accredited entity must ensure that advice is provided to individuals regarding how to safeguard their digital ID against cyber security risks.

(2) If an accredited entity is aware of a cyber security risk or cyber security incident in the digital ID system in which it operates and which is likely to adversely affect individuals, the entity must:

(a) where individuals interact directly with the entity's public facing DI data environment, provide information to individuals as to how to protect themselves from such risks or incidents; or

(b) where individuals do not interact directly with the entity's public facing DI data environment take reasonable steps to notify other relevant entities involved in the digital ID system of the incident, risk or breach.

Note: Subrule (b) – an example of not interacting directly with a DI data environment may include where the individual interacts with the relying party or a third-party during identity proofing.

4.9 Support to individuals

(1) An accredited entity must ensure that support services are provided to individuals who have been adversely affected by a cyber security incident. Support services must include, at a minimum, the provision of:

(a) a monitored chat or email function; and

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

Subdivision 1—System security plan

4.10 Requirement

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

(2) If an accredited entity implements ISO/IEC 27001 and ISO/IEC 27002 requirements, the system security plan:

(a) must include all documents and processes referred to in ISO/IEC 27001 and ISO/IEC 27002 which comprise the entity's 'information security management system' within the meaning of ISO/IEC 27001 and ISO/IEC 27002; and

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

(3) If an accredited entity implements the PSPF requirements, the system security plan:

(a) is the security plan referred to in PSPF Policy 11; and

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

Destruction of biometric information

(4) Where an accredited identity service provider collects, uses, holds, discloses or destroys biometric information—the system security plan must include the processes and procedures for the destruction of that biometric information

Assessment *of risks related to biometric information for accredited identity service providers*

(5) Where an accredited identity service provider collects, uses, holds, discloses or destroys biometric information—the system security plan must also include details of cyber security risks and associated mitigation strategies and treatments related to that biometric information, performing biometric binding, or biometric authentication including risks relating to:

(a) using biometric matching algorithms to complete biometric binding;

(b) using presentation attack detection systems to complete presentation attack detection;

(c) the capture, temporary storage, and destruction of biometric samples;

(d) the biometric matching process the entity implements;

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

(f) using manual processes performed by assessing officers to complete local biometric binding.

4.11 Review of the system security plan

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

(a) at least once in every 12-month period after its accreditation day; and

(b) as soon as practicable after:

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

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

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

(2) The review of the system security plan for subrule (1) must, at a minimum:

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

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

Note: If the entity implements the ISO27001 / ISO27002 requirements, subrule (2) may be met by the entity complying with clauses 8, 9 and 10 of ISO/IEC 27001.

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

Subdivision 2—Cloud service management

4.12 Selection, use and management of cloud services

(1) Where an accredited entity uses cloud services as part of its DI data environment, it must ensure that the use and management of those services is not inconsistent with these rules.

(2) An accredited entity must have and maintain a cloud services management plan.

(3) An accredited entity's cloud services management plan referred to in subrule (2) must include policies and processes for:

(a) the selection, use, and management of cloud services;

(b) defining and recording all relevant protective security requirements associated with the entity's use of cloud services;

(c) periodic security testing and assessment of assurance for the effective operation of relevant protective security requirements associated with the cloud services provider, including in relation to geographic location, management of privileged access and effective destruction of data;

(d) responding to cyber security incidents or suspected cyber security incidents involving the cloud services provider;

(e) the orderly migration of services and information from the cloud services provider;

(f) the approach to monitoring, reviewing and evaluating the ongoing use of cloud services to manage cyber security risks;

(g) whether digital ID information is to be collected, held, used or disclosed by the cloud service provider;

(h) how digital ID information is destroyed once it is no longer required; and

(i) amending or discontinuing the use of cloud services, including exit strategies for cloud services.

(4) An accredited entity must have and maintain a cloud services providers register which includes the following information:

(a) cloud services provider's name and cloud service name;

(b) purpose for using the cloud services;

(c) the type of digital ID information collected, used, held or disclosed by the cloud services provider;

(d) date for the next protective security assurance assessment of the cloud services;

(e) contractual arrangements for the cloud service; and

(f) contact details for the cloud service provider including emergency contact details.

Note: If the entity implements ISO/IEC 27001 and ISO/IEC 27002 (see paragraph 4.2(1)(a)), this rule 4.12 may be met by the entity complying with the requirements in control 5.23 of ISO/IEC 27001:2022.

Subdivision 3—Incident detection, investigation, response and reporting

4.13 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) The mechanisms referred to in subrule (1) must include a process for personnel, individuals, enforcement bodies and other entities to report actual or suspected cyber security incidents on a confidential basis.

4.14 Incident investigation, management and response

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

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

(3) The mechanisms referred to in subrule (1) must include processes and procedures to:

(a) manage and respond to cyber security incidents and suspected cyber security incidents; and

(b) for an accredited identity service provider:

(i) identify a digital ID that has been affected by a cyber security incident; and

(ii) suspend or prevent use of the digital ID; and

(c) for an accredited attribute service provider:

(i) identify attributes that have been affected by a cyber security incident; and

(ii) suspend or prevent use of the attributes.

4.15 Disaster recovery and business continuity management

(1) An accredited entity must have, maintain and comply with a disaster recovery and business continuity plan for its DI data environment that covers:

(a) business continuity governance;

(b) training requirements for recovery team members;

(c) recovery objectives and priorities;

(d) backup retention and protection from loss processes;

(e) backup recovery and restoration processes;

(f) continuity strategies; and

(g) testing requirements for restoration procedures.

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

(3) An accredited entity must at least once in every 12-month period after its accreditation day review and test its disaster recovery and business continuity plan.

Note: If the entity implements ISO/IEC 27001 and ISO/IEC 27002 (see subrule 4.2(1)(a)), this rule may be met by the entity complying with the requirements in controls 5.30 and 8.13 of ISO/IEC 27001:2022.

4.16 Record keeping

(1) An accredited entity must:

(a) keep records of decisions to use civil, administrative or disciplinary procedures, or to take no further action, in response to a cyber security incident; and

(b) keep records of the entity's investigation of and responses to cyber security incidents.

Subdivision 4—Information technology system controls

4.17 Essential Eight

(1) An accredited entity must implement and comply with the relative security effectiveness rating marked 'essential' in the Strategies to Mitigate Cyber Security Incidents document.

(2) For the purposes of this rule:

Strategies to Mitigate Cyber Security Incidents means the document titled 'Strategies to Mitigate Cyber Security Incidents' published by the ACSC.

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

4.18 Logging requirements

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

(2) An accredited entity must have and maintain a logging implementation and monitoring plan that details:

(a) how the entity provides, stores, protects, monitors and analyses logs;

(b) how the entity monitors logs for anomalous behaviour; and

(c) the activities, exceptions, faults and other relevant events in the entity's DI data environment.

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

(4) An accredited entity must comply with its logging implementation and monitoring plan.

Note: Subrules (2), (3) and (4) are equivalent to the requirements in ISO/IEC 27001, Annex A 8.15, 8.16 and 8.17.

(5) A log generated by an accredited entity in subrule (1) must also include the following details for each event:

(a) interaction type;

(b) transaction audit identifier;

(c) the names of the entities involved in the event;

(d) any unique identifier used in the event;

(e) for an accredited identity exchange provider—the types of attributes conveyed for the event; and

(f) for accredited entities other than an accredited identity exchange provider—the types of attributes requested and disclosed to the entities involved in the event.

(6) Each log as required by this rule must be retained for a minimum of 3 years from the date it was generated.

(7) An accredited entity must ensure logs do not contain biometric information.

(8) A log generated by an accredited entity as required by subrule (1) must include a record of:

(a) the creation, update, use, disclosure and destruction of digital ID information;

(b) the destruction of biometric information if collected or retained by or on behalf of the accredited identity service provider;

Accredited identity service providers

(c) for an accredited identity service provider, the binding of attributes to a digital ID;

(d) for an accredited identity service provider conducting biometric binding, information associated with each biometric binding transaction, in accordance with rules 5.17 to 5.25 including the biometric binding method used; and

(e) for an accredited identity services provider conducting manual face comparison activities:

(i) the manual face comparison activities undertaken during the biometric binding process;

(ii) the assessing officer(s) responsible for performing any activities related to the biometric binding transaction; and

(iii) whether or not technical verification of the claimed photo ID was completed as part of the biometric binding transaction.

Accredited attribute service providers

(f) for an accredited attribute service provider:

(i) the binding of attributes to a digital ID; and

(ii) the retrieval of attributes by a third party;

Logging requirements for accredited identity exchange providers

(g) for an accredited identity exchange provider:

(i) where the entity records consent on behalf of an identity service provider or attribute service provider, the duration of consent (including any time limit on the consent); and

(ii) the status of the consent provided by the individual such as 'grant', 'deny' or 'ongoing'.

4.19 Cryptography

(1) An accredited entity must ensure that all digital ID information collected, used, held or disclosed by or on behalf of the accredited entity is protected in transit and at rest by approved cryptography.

4.20 Cryptographic standards

(1) An accredited entity must comply with Transport Layer Security (**TLS**) 1.3 (within the meaning of the term in the ISM), unless the entity is unable to do so because TLS 1.3 is not supported by the device of an individual using the entity's accredited service.

Note: The cryptographic standards in the ISM includes a requirement to implement the latest version of TLS. As at the commencement of these rules, the current version of TLS is version 1.3.

(2) If an accredited entity is unable to comply with TLS 1.3, it must:

(a) implement at least TLS version 1.2; and

(b) follow relevant risk mitigation advice published by the ACSC in Implementing Certificates, TLS, HTTPS and Opportunistic TLS.

(3) In this rule:

Implementing Certificates, TLS, HTTPS and Opportunistic TLS means the document titled 'Implementing Certificates, TLS, HTTPs and Opportunistic TLS' published by the ACSC.

Note: At the commencement of these rules, 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

4.21 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 DI data environment and which cover cryptographic key lifecycle management, including:

(a) cryptographic key generation;

(b) registration;

(c) distribution;

(d) installation;

(e) usage;

(f) protection;

(g) storage;

(h) access;

(i) recovery; and

(j) destruction.

Note: If the entity implements ISO/IEC 27001 and ISO/IEC 27002 referred to in subrule 4.2(1)(a), this rule 4.21 may be met by the entity complying with control 8.24 in ISO/IEC 27001:2022 Annex A or with controls 10.1.1 and 10.1.2 of ISO/IEC 27001:2013.

Part 2—Fraud control requirements

Division 1—Capability

4.22 Fraud management capability

(1) ***Fraud management capability*** of accredited entity means the accredited entity's ability to manage fraud in its DI data environment in practice through the implementation and operation of processes and controls, including by:

(a) allocating adequate budget and resources; and

(b) providing for management oversight.

(2) An accredited entity's fraud management capability must be appropriate and adapted to respond to fraud risks, having regard to:

(i) the extent and nature of digital ID information that the entity holds;

(ii) the extent and nature of fraud risks, threats and vulnerabilities;

(iii) the potential loss or damage to one or more individuals if a digital ID fraud incident occurs;

(iv) the potential loss or damage to relying parties if a digital ID fraud incident occurs; and

(v) 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 rendered unreliable.

(3) An accredited entity must take reasonable steps to prevent, detect and deal with digital ID fraud incidents, including by:

(a) having and maintaining a fraud management capability;

(b) continuously improving its fraud management capability; and

(c) identifying, treating and managing fraud risks.

Division 2—Fraud controls

4.23 Fraud risk assessment

(1) An accredited entity must at least once in every 12-month period after its accreditation day, conduct an assessment of the fraud risks associated with its accredited services and DI data environment (***fraud risk assessment***).

(2) An 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 entity's risk matrix;

(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) Where an accredited identity service provider collects, uses, holds, discloses and destroys biometric information, the entity must assess and record in its fraud risk assessment the fraud risks, mitigation strategies and treatments related to that biometric information including the risks outlined in rule 0.

4.24 Sharing information about risks

(1) An accredited entity must:

(a) consider the implications that the entity's decisions related to the management of fraud risks have for other participants of the digital ID system in which the accredited entity operates; and

(b) share information on known fraud risks or digital ID fraud incidents with those participants where appropriate.

4.25 Fraud controller

(1) An accredited entity must have a key position of fraud controller held by a senior officer of the entity and who is given responsibility for:

(a) managing fraud risks; and

(b) facilitating the entity's compliance with the fraud control requirements specified in this Part.

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

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

4.26 Fraud awareness training

(1) An accredited entity must ensure that all personnel whose duties relate to its 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.

4.27 Advice to individuals

(1) An accredited entity must ensure that advice is provided to individuals regarding how to safeguard their digital ID against fraud risks.

(2) If an accredited entity is aware of a fraud risk or digital ID fraud incident in the digital ID system in which it operates and which is likely to adversely affect individuals, the entity must:

(a) where individuals interact directly with the entity's public facing DI data environment, provide information to individuals as to how to protect themselves from such risks or incidents; and

(b) otherwise, take reasonable steps to notify other relevant entities involved in the transaction in that digital ID system of the incident, risk or breach.

4.28 Support to individuals

(1) An accredited entity must ensure that support services are provided to individuals who have been adversely affected by a digital ID fraud incident. Support services must include, at a minimum, the provision of:

(a) a monitored chat or email function; and

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

Subdivision 1—Fraud control plan

4.29 Fraud control plan

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

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

Risks

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

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

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

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

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

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

Goals and strategic objectives

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

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

Personnel and training

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

Digital ID fraud incident management

(j) the strategies and controls for managing and investigating digital ID fraud incidents as required by subrule 4.32(3) and reporting digital ID fraud incidents to the Digital ID Regulator as per rule;

Destruction of biometric information

(k) where an accredited entity collects biometric information, the processes and procedures for the destruction of that biometric information

Biometric binding

(l) where an accredited identity service provider is performing biometric binding (see rules 5.17 to 5.25):

(i) details of the entity's approach to the use of biometric information referred to in rule 4.44;

(ii) details of the procedures implemented in subrule 5.25(6) to detect fraudulent activities conducted by assessing officers when performing manual face comparison referred to in subrule 5.25;

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

(iv) risks, threats and vulnerabilities specific to the entity's use of in-device biometric capability referred to in rule 5.62; and

(m) where biometric binding referred to in rules 5.17 to 5.25 applies in relation to an accredited identity service provider:

(i) risks, threats and vulnerabilities specific to the use of eIDVT in rule 5.24; and

(ii) processes and procedures to ensure the destruction of acquired images of processed photo IDs in accordance with these rules; and

(n) for an accredited identity service provider, the process undertaken by to meet the fraud control requirements referred to in Table 1 of rule 5.13.

Assessment of risks related to biometric information for accredited identity service providers

(1) Where an accredited identity service provider collects, uses, holds, discloses or destroys biometric information—the fraud control plan must also include details of digital ID fraud risks and associated mitigation strategies and treatments related to that biometric information, performing biometric binding, or biometric authentication including risks relating to:

(a) using biometric matching algorithms to complete biometric binding;

(b) using presentation attack detection systems to complete presentation attack detection;

(c) the capture, temporary storage, and destruction of biometric samples;

(d) the biometric matching process the entity implements;

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

(f) using manual processes performed by assessing officers to complete local biometric binding.

4.30 Review of the fraud control plan

(1) An accredited entity must review and update its fraud control plan:

(a) at least once in every 12-month period after its accreditation day; and

(b) as soon as practicable after:

(i) the entity becomes aware of a digital ID fraud incident which is of a type 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 a breach of the requirements of its fraud control plan; or

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

(2) The review of the fraud control plan in subrule (1) must, at a minimum:

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

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

(c) review and, where necessary, update the goals and strategic objectives in its fraud control plan:

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

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

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

(4) All changes to the fraud control plan referred to in subrule (3) must be approved by the accredited entity's fraud controller.

Subdivision 2—Incident detection, investigation, response and reporting

4.31 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) The mechanisms referred to in subrule (1) must include a process for personnel, individuals, enforcement bodies and other entities to report digital ID fraud incidents on a confidential basis.

4.32 Investigation, management and response

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

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

(3) An accredited entity must implement and maintain mechanisms for responding to digital ID fraud incidents, including, procedures to:

(a) document the entity's processes for responding to digital ID fraud incidents and how it will investigate such incidents; and

(b) include appropriate criteria for making timely decisions at each critical stage in response to a digital ID fraud incident.

(4) If an accredited entity cannot investigate digital ID fraud incidents in accordance with subrule (1) because the entity does not hold personal information, the entity must take reasonable steps to assist with fraud investigations being carried out by other entities within the same digital ID system.

Note: For subrule (4), reasonable steps may include the provision of relevant information to another entity.

4.33 Record keeping

(1) An accredited entity must:

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

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

Part 3—Privacy

Division 1—Requirements

4.34 Interpretation

(1) In this Division:

privacy governance code means the *Privacy (Australian Government Agencies — Governance) APP Code 2017* or an instrument that replaces that code.

4.35 Compliance with privacy governance code

(1) In this rule:

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

(2) For an accredited entity which is not an agency within the meaning of that term in the Privacy Act, the entity must comply with the privacy governance code in respect of its DI data environment and accredited services as if the entity were an agency for the purposes of the code.

Note 1: 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.

Note 2: The Information Commissioner is the regulator for the additional privacy safeguards in Part 2, Division 2 of Chapter 3 of the Act. The Digital ID Regulator may seek the advice of the Information Commissioner in relation to privacy matters (see section 40 of the Act).

4.36 Privacy policy

(1) An accredited entity must have and maintain a privacy policy covering its DI data environment and accredited services which is separate to the privacy policy for its other business or organisational functions.

(2) An accredited 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; or

(b) distinct sections in its privacy policy and privacy management plan for each kind of accredited entity.

4.37 Review

(1) An accredited entity must at least once in every 12-month period after its accreditation day, review its privacy policy and privacy management plan, as required by the privacy governance code.

4.38 Data minimisation principle

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

(2) An accredited entity must only disclose personal information to a relying party or participating relying party if it is satisfied that disclosure of that personal information to that party is reasonably necessary for that party to:

(a) provide its service; or

(b) enable an individual to access its service.

(3) Subrule (2) also applies where the entity and the relying party or participating relying party are the same entity.

(4) An accredited entity will satisfy its obligations referred to in subrule (2) if it has processes in place to verify that the personal information sought by a relying party or participating relying party is reasonably necessary for the activities in that subrule.

4.39 Disclosure for fraud activities

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

4.40 Privacy awareness training

(1) An accredited entity must ensure that each of its personnel whose duties relate to its DI data environment or accredited services completes privacy awareness training involving its privacy policy, privacy management plan and compliance with the privacy requirements in Chapter 3 of the Act and these rules:

(a) before starting work on those duties; and

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

4.41 Data breach response plan

(1) An accredited entity must have and maintain 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.

(2) The data breach response plan must:

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

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

(i) escalated within the entity;

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

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

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

(3) An accredited entity must review and update its data breach response plan at least once in every 12-month period after its accreditation day.

4.42 Record keeping

(1) An accredited entity must:

(a) keep records of 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 responses to data breaches.

Division 2—Retention and use of biometric information

4.43 Requirements

(1) For the purposes of paragraph 46(5)(d) of the Act, an accredited entity that retains biometric information of an individual for the purpose of undertaking testing in relation to the information must comply with the requirements of this rule.

Note: The biometric information must be destroyed no later than 14 days after it was collected—see paragraph 48(3)(b) of the Act.

Purposes for which tests may be conducted

(2) An accredited entity may undertake testing using biometric information only for one or more of the following purposes:

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

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

(c) to optimise the presentation attack detection technology to improve its usability;

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

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

(f) to optimise controls that account for variances in image quality; 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) by a person qualified to conduct the testing; and

(b) in accordance with:

(i) the entity's system security plan;

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

(iii) a testing plan that complies with subrule (5) .

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

(5) The test plan must include:

(a) the objectives of the testing;

(b) the methodology to be used to conduct testing, including a description of the biometric information and the sample sizes to be used to conduct the testing;

(c) the test frequency and duration of testing; and

(d) how the biometric information will be stored and destroyed during the period of the testing.

Reporting of test results

(6) The entity must report the results of the testing to the Digital ID Regulator as part of its annual review.

(7) The results must include the following information for the previous 12-month period:

(a) the total number of transactions that occurred where biometric information was collected;

(b) the number of transactions tested;

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

(d) whether the testing has resulted in the entity taking action to respond to issues arising from the testing; and

(e) an assessment of whether the retention, use and disclosure of biometric information for testing continues to be an effective risk-mitigation measure, commensurate with the risk of the entity undertaking such testing.

Note: For example, the entity's assessment could include consideration of whether tests using biometric information has improved the thresholds of the presentation attack detection system to effectively reject malicious actors.

4.44 Requirements in relation to retention and use of biometric information— digital ID fraud incidents

(1) For the purposes of section ^46(7) of the Act, an accredited entity that retains biometric information of an individual for the purposes of preventing or investigating a digital ID fraud incident must conduct those fraud-related activities in accordance with written ethical principles aimed at avoiding disadvantage to, or discrimination against, individuals.

Note: The biometric information must be destroyed no later than 14 days after it was collected—see subsection ^48(4) of the Act.

Part 4—Usability and accessibility requirements

4.45 Interpretation

(1) In this Part:

public-facing information related to accredited services means information made available by the accredited entity in relation to an accredited entity's public-facing accredited services.

Note: An example of public facing information related to accredited services is the accredited entity's privacy policy made available to individuals.

public-facing accredited services means the accredited services or elements of an accredited entity's DI data environment an individual directly interacts with when using or attempting to use the entity's accredited services.

Note: An example of public-facing accredited services could be where an individual provides information to be verified as part of the identity proofing process via an accredited identity service provider's mobile app that individuals download and use to access the accredited services.

4.46 Usability and accessibility capability

(1) An accredited entity must take reasonable steps to continuously improve the usability and accessibility of its public-facing accredited services and public-facing information related to its accredited services so as to assist individuals.

4.47 Accessibility requirements for all accredited entities

(1) An accredited entity must:

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

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

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

(2) An accredited entity must take reasonable steps to ensure public-facing accredited services and public-facing information related to its accredited services meets WCAG version 2.1 to the AA standard.

4.48 Usability and Accessibility support

(1) An accredited entity with public-facing accredited services must:

(a) provide assisted digital support to individuals who are unable to use the entity's DI data environment independently and notify individuals of such support; and

(b) notify individuals of alternative channels (if any) made available by the entity for individuals to obtain the benefit of the entity's accredited services\.

Note 1: For subrule (a), assisted digital support may include for example, a monitored email address, a chat function or a call centre.

Note 2: For subrule (b), alternative channels may include for example, an in-person shopfront.

(2) An accredited entity with public-facing accredited services must take reasonable steps, including having processes and procedures, to:

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

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

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

4.49 Journey map

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

(2) The journey map must:

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

(b) depict the stages and interfaces an individual will go through when interacting with the entity's DI data environment;

(c) detail alternative channels (if any) available to the individual to complete a specific activity; and

(d) be included in the entity's privacy management plan.

Part 5—Reportable incidents

4.50 General

(1) This Part applies to an accredited entity providing services in a digital ID system other than the Australian Government Digital ID System.

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

4.51 Reportable incidents

(1) An accredited entity must notify the Digital ID Regulator within 7 days if any of the following occurs:

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

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

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

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

Note: In relation to subrule (c), the Digital ID Rules prescribe matters to which the Digital ID Regulator must have regard when considering whether an entity is a fit and proper person for the purposes of the Act and these rules.

4.52 Change of control for corporations

(1) In this rule:

corporation has the meaning given in the *Corporations Act*.

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

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

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

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

(2) For an accredited entity that is a corporation, the entity must notify the Digital ID Regulator, in accordance with this rule, of a change in control (within the meaning of section 910B of the *Corporations Act*), or a proposed change of control.

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

(a) the name of the incoming entity;

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

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

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

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

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

(g) in respect of each subsidiary of the incoming entity—the information specified in subrules (a) to (f); and

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

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

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

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

Chapter 5 Role requirements for accredited entities

Part 1—Preliminary

5.1 Interpretation

(1) In this Chapter:

ASP means an accredited attribute service provider.

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

authentication level means the level of assurance specified in Table 2 of rule 5.45.

authentication management means a service that does either or both of the following:

(a) generates, binds, manages and distributes authenticators to an individual; and

(b) binds, manages or distributes authenticators generated by an individual.

authenticator binding means the process of linking an authenticator with a digital ID.

authoritative source means an entity that issues attributes or credentials that relate to an individual.

document liveness means the presence of the original physical document.

false match rate has the same meaning as in ISO 2382-37.

ISP means an accredited identity service provider.

IXP means an accredited identity exchange provider.

liveness detection means the measurement and analysis of biometric, biological and behavioural characteristics or involuntary or voluntary reactions of the live presentation of the 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.

one-off digital ID means a digital ID generated and verified for the purpose of a one-time use.

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

presentation attack instrument species means a class of presentation attack instrument created using a common production method and based on different biometric characteristics.

public key means the cryptographic key in an asymmetric cryptographic key pair which may be made public.

session termination event means the event that brings an 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.

single logout means the ability for an individual to initiate a logout process for all relying parties that relied on a single logon session for the individual at an IXP.

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

source verification means the process of verifying an attribute or credential with the authoritative source (or a service that confirms the veracity of the attribute or credential with an authoritative source, such as the Document Verification Service).

Part 2—Accredited identity service providers

5.2 Digital IDs and children

(1) An ISP must not generate, manage, maintain or verify information of an individual if the individual has not yet attained the age of 15 years.

(2) An ISP must not generate, bind, manage or distribute authenticators to an individual if the individual has not yet attained the age of 15 years.

Consultation note: it is proposed to change this rule to individuals of 14 years to maintain consistency with other schemes. This is subject to consultation feedback and compliance with the Age Discrimination Act.

Division 1—Requirements for one-off digital IDs

5.3 One-off digital IDs

(1) When generating and verifying a one-off digital ID, an ISP must comply with Division 3 of this Part.

(2) However, the ISP is not required to comply with items 1 and 2 of Table 1 of rule 5.13.

(3) The ISP must not retain an attribute of an individual once disclosed to the relying party other than as required by law.

Division 2—Requirements for reusable digital IDs

5.4 Application

(1) This Division applies to an ISP that is generating, managing, maintaining or verifying a reusable digital ID.

5.5 Authentication and identity proofing management

(1) When generating and verifying a reusable digital ID, an ISP must comply with Division 3 of this Part.

(2) The ISP must bind the digital ID to an authenticator that meets the requirements of the authentication management standard in Part 4 of this Chapter for that digital ID.

5.6 Attribute management

(1) The ISP must allow an individual to update and correct the attributes of the individual held by the ISP.

(2) Before binding the new or updated attribute to the individual's digital ID, the ISP must:

(a) require the individual to authenticate to the authentication level bound to the digital ID; and

(b) verify the attribute as required by Table 1 of rule 5.13.

(3) The ISP must undertake verification of a linking credential (see Table 2 of Schedule 1) if an individual's attributes vary across credentials in accordance with the requirements in Table 1 of rule 5.13.

5.7 Suspension and deactivation of a digital ID

(1) If an individual requests the ISP to suspend or deactivate 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:

(i) suspend the use of the digital ID for the period requested; or

(ii) deactivate the digital ID; and

(c) following a suspension, notify the individual of the process to reactivate the digital ID.

Note 1: Subrule (a) – the controls in place to assist an accredited entity to confirm the legitimacy of the request must be addressed in the entity's fraud control plan—see rule 4.29.

Note 2: See subrule 5.11(2) for the process to reactivate a digital ID.

(2) If the ISP suspends an individual's digital ID at the direction of the Digital ID Regulator, the ISP must provide a process for the individual to reactivate the digital ID.

Note: See subrule 5.11(2) for the process to reactivate a digital ID.

(3) Promptly after suspending or deactivating a digital ID, an accredited entity must:

(a) notify the individual in writing that their digital ID has been suspended or deactivated;

(b) provide the reason for the suspension or deactivation; and

(c) if the digital ID has been suspended, notify the individual of the process to reactivate the digital ID.

Note: See rule 5.11 for the process to reactivate a digital ID.

5.8 Management of a suspected digital ID fraud incident or cyber security incident

(1) Where the registration 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 relevant digital ID has not been compromised; and

(b) take reasonable steps to verify and confirm that the individual has effective control of their digital ID.

(2) If the ISP has taken reasonable steps in accordance with subrule 5.8(1)(b), but has not been able to verify and confirm that the individual has effective control of their digital ID, the ISP must suspend the digital ID.

(3) To reactivate a digital ID that has been suspended due to a suspected digital ID fraud incident or suspected cyber security incident, an accredited entity must follow the process set out in subrule 5.11(1).

5.9 Management of a digital ID fraud incident or cyber security incident of a digital ID

(1) If the ISP detects a digital ID fraud incident or cyber security incident in relation to an individual's digital ID, the ISP must suspend that digital ID.

(2) To reactivate a digital ID that has been suspended due to a digital ID fraud incident or cyber security incident, an accredited entity must follow the process set out at subrule 5.11(1)5.11.

5.10 Expiry of a reusable digital ID

(1) For a digital ID proofed to level IP1 Plus or IP2, the digital ID will expire where an individual has not verified a credential listed in Schedule 1 in accordance with Division 3 of this Part for a period of 5 years.

(2) For a digital ID proofed to IP2 Plus, IP3 and IP4, the digital ID will expire where an individual has not completed biometric binding in accordance with Division 3of this Part for a period of 5 years.

5.11 Reactivation of a digital ID

(1) If the digital ID has been suspended as a result of a suspected or actual cyber security incident or digital ID fraud incident, to reactivate the digital ID, an accredited entity must ensure that:

(a) the individual completes the identity proofing process for the identity proofing level of the digital ID; and

(b) the attributes presented as part of the identity proofing process for the identity proofing level can be linked to the attributes which comprise the digital ID.

(2) If the digital ID has been suspended as a result of a request of an individual or the Digital ID Regulator, to reactivate the digital ID, an accredited entity must ensure that:

(a) the individual completes the identity proofing process for the identity proofing level of the digital ID and ensure that the attributes presented can be linked to the attributes which comprise the digital ID; or

(b) the individual completes biometric binding in accordance with the requirements in Subdivision 2 of Division 3 of this Part using a credential whose attributes can be linked to the current attributes which comprise the digital ID.

(3) The ISP will not be required to reactivate a digital ID where the ISP no longer retains the relevant information to comply with subrules (1) and (2).

5.12 Step-up of identity proofing for reusable digital IDs

(1) The ISP may allow an individual to step up an existing identity proofing level to a higher identity proofing level in accordance with this rule.

(2) The ISP must not step-up the identity proofing level of an individual's digital ID to a higher identity proofing level unless:

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

(b) 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 of Table 1 of rule 5.13 for the digital ID; and

(c) the individual's digital ID meets all the requirements of the higher identity proofing level as required by Table 1 of rule 5.13.

(3) When the step-up process is completed, the ISP must notify the individual of the new proofing level for the individual's digital ID.

Division 3—Identity proofing standards for digital IDs

5.13 General

(1) When generating and verifying a digital ID, an ISP must comply with this Division.

(2) The ISP must only conduct identity proofing on a credential listed in Schedule 1.

(3) The ISP must ensure that it complies with the requirements specified as 'must' or 'yes' in Table 1 in this Division for the relevant identity proofing level.

(4) For the purposes of items 10 (verification of a COI credential) and item 11 (verification of a photo ID) in Table 1 in this Division, Australian passports and Australian ePassport may only be used as a single credential to satisfy the requirements for verification of a COI and photo ID up to the level of IP3.

(5) For the purposes of item 10 in Table 1 in this Division (verification of a COI credential)—the ISP must not accept an Australian passport as the COI credential when identity proofing at the level of IP4.

Table 1: Identity proofing levels and requirements for each level

Item	Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
	Uniqueness objective *Note: ISPs providing identity proofing for one-off digital IDs are not required to comply with the uniqueness objective requirements at items 1 and 2 – see rule 5.3.*						
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
	Legitimacy objective						
3	A check undertaken by the ISP that the identity is not that of a deceased person	—	Recommended	Recommended	Recommended	Must	Must
	Binding objective						
4	Verification of the link between the individual and the claimed identity to occur through biometric binding in accordance with the requirements set out in Subdivision 2, Division 3 of Part 2 of this Chapter	—	—	—	Must	Must	Must
5	All original, physical credentials to be provided and the individual witnessed in-person	—	—	—	—	—	Must

Item	Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
	Fraud control objective						
6	Checks to be undertaken against information or records held within the ISP to confirm the identity is not known to be used fraudulently.	—	Must	Must	Must	Must	Must
	Other Requirements						
7	Personnel undertaking identity proofing processes, including visual verification, are required to be provided with tools and training to detect fraudulent attributes and credentials before starting working on these duties and annually thereafter.	—	Must	Must	Must	Must	Must
8	NAATI accredited translation of credentials in languages other than English required?	—	—	Recommended	Recommended	Must	Must
9	Attributes that must be verified using source verification or technical verification.	—	All names Date of birth	All names Date of birth	All names Date of birth	All names Date of birth	All names Date of Birth
	Credentials required for verification						
10	Verification of a COI credential must be undertaken?	—	—	Yes, unless photo ID used (see item 11).	Yes, unless photo ID used (see item 11).	Yes	Yes
11	Verification of a photo ID must be undertaken?	—	Yes, unless UiTC credential used (see item 12).	Yes, unless COI credential used (see item 10).	Yes, unless COI credential used (see item 10).	Yes	Yes

Item	Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
12	Verification of a UiTC credential must be undertaken?	—	—	Yes x 1	Yes x 1	Yes x 1	Yes x 2
13	Verification of a linking credential must be undertaken if attributes vary across credentials?	—	—	Yes	Yes	Yes	Yes
14	Approved authenticator bindings	AL1/AL2/AL3	AL2/AL3	AL2/AL3	AL2/AL3	AL2/AL3	AL3

Note 1: The checks undertaken by the ISP for the purposes of item 2 in Table 1 may be done through checking existing records of the ISP for a digital ID with the same attributes.

Note 2: The checks undertaken by the ISP for the purposes of item 6 in Table 1 may include checks against the ISP's registers of known fraudulent identities.

Note 3: For the purpose of item 8, NAATI refers to the National Accreditation Authority for Translators and Interpreters. Further information is available at https:///www.naati.com.au/

Note 4: For the purposes of item 9 in Table 1, all names and date of birth of the individual must be verified as part of the identity proofing process, meaning at least one of the presented credentials must have those attributes available to be verified.

Subdivision 1—Verification rules

5.14 Source verification

(1) Where an accredited entity is conducting source verification of a credential or attribute:

(a) listed in Schedule 1 (where the entity is an ISP); and

(b) that is not issued by a government entity,

the entity must carry out source verification by:

(c) establishing a trusted and secure connection with the authoritative source using approved cryptography;

(d) ensuring that the authoritative source can verify that the credential or attributes being verified are current; and

(e) ensuring that all checks required in the description of the credential in Schedule 1 are carried out to complete source verification.

5.15 Technical verification

(1) Where an accredited entity is performing technical verification of a credential or attribute other than an ePassport, the entity must:

(a) have and maintain a business process to establish a technical process using public key infrastructure technology to prove that a particular certificate originates from a trusted source and is valid (***chain of trust***);

(b) use the chain of trust to verify:

(i) where the entity is an ISP, that the credential has been issued by an issuer listed in Schedule 1;

(ii) where the entity is an ASP, that the credential or attribute has been issued by an issuer established as trusted by the business process set out at subrule (a); and

(iii) in all cases, that the credential or attribute has not been revoked by the issuer;

(c) comply with the verification terms of use set by the issuer of the credential or attribute;

(d) ensure that its technical verification process includes a requirement to confirm that the credential or attribute:

(i) is valid; and

(ii) has not been tampered with or modified; and

(e) where a certificate revocation list, within the meaning of that term in document RFC 5280, is available, establish that the credential or attribute has not been revoked.

Note: For document RFC 5280, see: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (available at https://datatracker.ietf.org/doc/html/rfc5280)

(2) Where an accredited entity is performing technical verification on an ePassport, the entity must:

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

(b) without limiting subrule (a), ensure that where a certificate revocation list is available, establish that the ePassport has not been revoked.

5.16 Visual verification

(1) The ISP must not attempt visual verification of a credential presented by an individual unless the credential:

(a) is listed in Schedule 1; and

(b) cannot be verified by source verification or technical verification.

Subdivision 2—Biometric binding

5.17 Interpretation

(1) In this Subdivision:

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.

image quality profile is 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.

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

5.18 Application

(1) This Division applies to an ISP that is conducting identity proofing at levels IP2 Plus, IP3 and IP4.

5.19 General requirements for biometric binding

(1) The ISP must complete biometric binding by performing either:

(a) online biometric binding in accordance with rule 5.20; or

(b) local biometric binding in accordance with rule 5.21.

(2) The ISP must perform source verification of a photo ID that is used in the biometric binding process as part of biometric binding in accordance with rule 5.23.

(3) Where the photo ID used is a foreign passport, the ISP must ensure that the foreign passport is linked to a current visa by performing source verification.

5.20 Online biometric binding

(1) For online biometric binding, an ISP must comply with this rule.

(2) To complete online biometric binding, an ISP must capture an acquired image and perform at least one of the following on the image:

(a) technical biometric matching in accordance with rule 5.22;

(b) source biometric matching in accordance with rule 5.23; or

(c) eIDVT biometric matching in accordance with rule 5.24.

(3) The ISP must not use an acquired image for biometric binding unless:

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

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

(4) The ISP must take into account the characteristics of biometric image quality described by ISO 29794-5 when generating the image quality profile of the acquired image.

(5) The ISP must record evidence of the characteristics used in generating the image quality profile, which may include:

(a) evidence in technical documents;

(b) demonstrations of the service in action; and

(c) the internal quality assurance processes.

(6) The ISP must include automated quality controls and 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.

(7) The ISP must complete online biometric binding in a single continuous workflow.

Use of presentation attack detection and liveness detection

(8) The ISP must include liveness detection as part of presentation attack detection.

(9) The ISP must incorporate presentation attack detection at the point of capture of the acquired image.

(10) The ISP must complete the capture of the acquired image and presentation attack detection, as part of the same process, before the acquired image is submitted for biometric binding.

(11) The ISP must employ presentation attack detection based on data captured by both the data capture subsystem and through system level monitoring, as described by ISO 30107-1.

5.21 Local biometric binding

(1) For local biometric binding, an ISP must comply with this rule.

(2) Local biometric binding must be performed by an assessing officer in the physical presence of the individual using one or more of the following processes:

(a) technical biometric matching in accordance with rule 5.22;

(b) source biometric matching in accordance with rule 5.23; or

(c) eIDVT biometric matching in accordance with rule 5.24; or

(3) However, if all biometric information processed for subrule 5.21(2) is unavailable or unable to be completed, manual face comparison in accordance with rule 5.25.

(4) While performing local biometric binding, the ISP must restrict access to biometric information and the biometric capability of the ISP to the assessing officers.

(5) If an acquired image is being captured as part of local biometric binding, the ISP must develop and apply an image quality profile in accordance with rule 5.20.

(6) The ISP must undertake local biometric binding only at a location identified in its fraud control plan and system security plan.

5.22 Technical biometric matching

(1) For technical biometric matching, an ISP must implement and maintain the requirements of this rule.

(2) Where the ISP acquires an image from an credential listed in Table 4 of Schedule 1 (Photo IDs) to conduct technical biometric matching, the ISP must verify the authenticity of the credential and image using the relevant technical verification process in rule 5.15.

(3) The ISP must only process photo IDs through technical biometric matching that are government issued.

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

5.23 Source biometric matching

(1) For source biometric matching, an ISP must comply with this rule.

(2) To perform online biometric binding with source biometric matching, the ISP must:

(a) identify an authoritative source capable of performing source biometric matching of the relevant photo ID;

(b) provide the acquired image to the authoritative source to perform source biometric matching to verify that the individual's acquired image biometrically matches the corresponding photo ID image stored by the authoritative source;

(c) provide the authoritative source with other information about the photo ID required by the authoritative source to perform source biometric matching; and

(d) obtain verification from the authoritative source that the individual's acquired image biometrically matches the corresponding photo ID image stored by the authoritative source.

5.24 eIDVT biometric matching

(1) For the purposes of this rule:

identity document template means a model representation of a particular identity document that is used to verify an acquired image of an identity document of that type. The identity document template may include, but is not limited to, text locations, colours and other graphical elements, security features, and locations of facial biometrics for identity documents that are also photo IDs.

(2) For eIDVT biometric matching an ISP must comply with this rule.

(3) The ISP must only perform eIDVT biometric matching using the following physically presented photo IDs:

(a) Australian driver licences;

(b) Australian passports; or

(c) Australian ePassports.

(4) The ISP must ensure that its eIDVT includes processes to:

(a) identify and verify that the physically presented photo ID 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 credential, and not a second-generation image such as an image of an image of a credential or a photocopy of a credential.

(5) the ISP must only process photo IDs through eIDVT that are:

(a) successfully verified as authentic; and

(b) determined by the entity as having been physically present at the time of capture by testing for document liveness (see rule 5.31).

(6) When processing a photo ID through eIDVT, the entity must ensure that the eIDVT:

(a) identifies at least five security features in the photo ID and compares the security features against an identity document template;

(b) compares the photo ID's expiry date to the date on which the matching is attempted;

(c) ensures the facial image on the photo ID is genuine and has not been altered, changed or modified in any way;

(d) only processes images with a resolution of at least 300 dpi; and

(e) limits the number of attempts to verify the authenticity of a photo ID using eIDVT to five.

(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 up to 14 days for the purposes of fraud investigation as part of a digital ID fraud incident.

(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; and

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

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

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

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

5.25 Manual face comparison

(1) When performing manual face comparisons, an ISP must comply with this rule.

(2) The ISP must only perform manual face comparison using an original, physical, photo ID (see Table 4 of Schedule 1) presented in person by the individual at the time the manual face comparison is performed.

(3) The ISP must only attempt manual face comparison if the photo ID presented for biometric binding is unable to be processed using the following processes:

(a) technical biometric matching—see rule 5.22;

(b) source biometric matching—see rule 5.23; or

(c) eIDVT biometric matching—see rule 5.24.

(4) The ISP must ensure that the ISP's assessing officer performing manual face comparison receives awareness training in accordance with the guidance provided by the latest version of *Guide for Facial Comparison Awareness Training of Assessors* published by the Facial Identification Scientific Working Group:

(a) before starting to perform manual face comparisons for the ISP; and

(b) at least once in every 12 months thereafter.

(5) The ISP must provide assessing officers with a current reference document outlining practical steps and guidance when performing manual face comparison.

(6) The ISP must implement and maintain procedures to detect any fraudulent activities conducted by assessing officers when performing manual face comparison.

Note: Details of these procedures must be included in the accredited entity's fraud control plan—see rule 4.29.

(7) The ISP must:

(a) implement and maintain quality control and quality assurance procedures for manual face comparison decisions made by assessing officers; and

(b) record these procedures in its cyber security plan and fraud control plan referred to in rules 4.10 and 4.29.

Subdivision 3—Biometric testing

5.26 Interpretation

(1) In this Subdivision:

document false accept rate means the proportion of document verification transactions with credential fraud that are incorrectly confirmed as authentic.

document false reject rate means the proportion of genuine document verification transactions with truthful claims of a genuine document that are incorrectly denied.

document fraud attack means the techniques used to create fraudulent documents. Techniques can be digital or physical and can include document tampering or creation of a counterfeit document.

document fraud instrument means an object or image used in a credential fraud attack (for example, a forged or counterfeit photo ID).

document fraud instrument species means a class of document attack instruments created using a common production method and based on different persons.

FIDO document authenticity verification requirements means the requirements developed by FIDO (Fast Identity Online) for testing eIDVT solutions.

Note: At commencement of these rules, located at: https://fidoalliance.org/specs/idv/docauth/document-authenticity-verification-requirements-v1.0-fd-20220815.html

test set has the definition given to the term in section 6.2 of the FIDO document authenticity verification requirements.

5.27 Biometric testing entity

(1) If an accredited entity is required to have biometric testing carried out by a biometric testing, the entity must engage a biometric testing entity that meets the requirements of this rule.

(2) The biometric testing entity must:

(a) use appropriately experienced personnel with a background in biometric testing to conduct the biometric testing;

(b) be or use a laboratory certified under ISO 17025;

(c) have a policy for working with human test subjects that has been approved by a relevant national body;

(d) have established test methods for:

(i) presentation attack detection testing informed by ISO/IEC 30107-3, if performing testing for rule 5.28; and

(ii) biometric matching algorithm accuracy testing informed by ISO/IEC 19795-2, if performing testing for rule 5.29; and

(e) be independent from the design, implementation, operation and management of the entity's DI data environment and accredited services and be:

(i) external to the entity; or

(ii) if the entity is part of a group, external to the group.

(3) For eIDVT testing required for rules 5.31 and 5.32, the biometric testing entity must meet the requirements in subrule (2) and must:

(a) be a FIDO Accredited Laboratory as defined by the FIDO document authenticity verification requirements;

(b) use appropriately experienced personnel with a background in document and eIDVT testing to conduct the eIDVT testing; and

(c) have implemented policy and procedures that demonstrate the biometric testing entity's responsible management and storage of physical document fraud instruments.

Note: An entity accredited to perform presentation attack detection testing according to ISO/IEC 30107-3 and/or biometric performance testing according to ISO/IEC 19795-2 under the National Voluntary Laboratory Accreditation Program coordinated by the National Institute of Standards and Technology ordinarily would meet the above requirements in subrule (2)(d) for each kind of testing respectively.

5.28 Testing of presentation attack detection technology

(1) In this rule:

level A presentation attack instrument species means a category of presentation attack instruments which:

(b) have an elapsed creation time equal to or less than one day;

(c) can be created or undertaken by a layperson;

(d) can be undertaken with standard equipment; and

(e) involves a source of biometric information which is easy to obtain such as a photo from social media or voice recording.

level B presentation attack instrument species means a category of presentation attack instruments which:

(a) have an elapsed creation time equal to or less than seven days;

(b) can be created or undertaken by a person who has the required expertise to do so;

(c) can be undertaken with standard or specialised equipment; and

(d) involves a source of biometric information which is moderately difficult to obtain such as a stolen fingerprint image or voice recording of a specific phrase.

(2) If an entity conducts online biometric binding, it must ensure its presentation attack detection technology is tested by a biometric testing entity in accordance with the requirements:

(a) specified in ISO 30107-3; and

(b) of this rule.

(3) The testing of the presentation attack detection technology must:

(a) be performed on a system that incorporates all hardware and software involved in the entity's biometric binding process;

(b) be performed using configurations and settings that align to the entity's DI data environment;

(c) calculate and record the completed presentation attack detection evaluation and corresponding results for each presentation attack instrument species as those artefacts and process for testing are defined by ISO 30107-3, and that covers rule 5.28;

(d) include presentation attack instrument species to address potential presentation attack threats, as informed by the risk assessment required by rule 4.5;

(e) include at least 6 level A presentation attack instrument species and at least 6 level B presentation attack instrument species; and

(f) include a minimum of 10 individuals.

(4) The ISP must obtain a copy of the testing report from the testing entity confirming that the entity's presentation attack detection technology has been tested in accordance with the relevant requirements of ISO 30107-3 and this rule.

(5) The ISP must ensure that for each presentation attack instrument species at least one presentation attack instrument is created covering a minimum of 3 individuals and is included in the testing.

(6) All presentation attack instrument species used in testing must have an attack presentation classification error rate (***APCER***) of 0%.

(7) If the reported APCER for any presentation attack instrument species does not meet the requirements of subrule (6), the biometric testing entity must prepare a risk-based justification for such failures that includes:

(a) supplementary testing on presentation attack instrument species that failed the requirement;

(b) a qualitative assessment of whether the entity's presentation attack detection technology is fit for purpose for its biometric vulnerability landscape; and

(c) confirm this meets the requirements of these rules.

5.29 Testing of biometric matching algorithm

(1) If an entity conducts technical biometric matching in accordance with rule 5.22 or eIDVT biometric matching in accordance with rule 5.24, the entity must ensure its biometric matching algorithm is tested by a biometric testing entity, in

accordance with the testing and reporting specifications described in ISO/IEC 19795-2 to determine the:

(a) failure to enrol rate;

(b) failure to acquire rate;

(c) false match rate; and

(d) false non-match rate.

(2) The biometric matching algorithm must be tested using operational configurations and settings that are consistent with and align to the entity's operating environment.

(3) The biometric matching algorithm must be tested using representation from a diverse age, gender, and ethnicity demographics that considers possible individuals who may use the entity's accredited services.

(4) The biometric matching algorithm testing must establish, with a minimum 90% confidence interval, that the algorithm achieves a false match rate of not more than 0.01% and a false non-match rate of not more than 3%, as described in ISO/IEC 19795-9.

(5) The ISP must provide the Digital ID Regulator with a copy of the report from the biometric testing entity confirming that the entity's biometric matching algorithm has been tested in accordance with the relevant testing and reporting specifications described in ISO/IEC 19795-2 and as required by this rule.

5.30 Source biometric matching testing

(1) If an entity conducts source biometric matching, the entity must provide the Digital ID Regulator with evidence that end-to-end testing has been undertaken between the entity's biometric capability and the authoritative source, to ensure the entity's biometric capability meets any operating standards set by the authoritative source for biometric matching.

5.31 Testing for document liveness

(1) In this rule:

levels A, B, C, and D, in relation to document fraud attacks, have the definitions given to those terms in section 6.2.1.2 of the FIDO document authenticity verification requirements.

(2) If an entity conducts eIDVT biometric matching in accordance with rule 5.24, the entity must ensure its biometric matching algorithm is tested by a biometric testing entity in accordance with this rule.

Inputs for digital testing

(3) For digital testing, the entity must either use:

(a) 300 images of documents for each test set as per section 6.2 of the FIDO document authenticity verification requirements; or

(b) 300 instances of the inputs the eIDVT uses to detect document liveness that include but are not limited to the following:

(i) short video;

(ii) two or more separate images usually at different angles or of the reverse of the document; or

(iii) some other challenge or response as required by the technical specifications of the eIDVT testing.

Evaluations with document fraud instruments

(4) The test set of document fraud instruments must:

(a) comply with the conditions imposed by section 6.3.2 of the FIDO document authenticity verification requirements; and

(b) contain:

(i) at least 10% of document fraud instruments at level A, B, and C shall be genuine second-generation document images; and

(ii) no documents that are considered to be out-of-scope for processing through the eIDVT.

Levels of document fraud attacks in scope for physical testing

(5) In relation to an entity's physical testing of document fraud instruments, the following levels of document fraud attack are within scope:

(a) level A attacks; and

(b) level B attacks.

Test set conditions for physical evaluation using document fraud instruments

(6) The test set of document fraud instruments used for physical testing must include:

(a) a minimum of 100 document fraud instruments which reasonably covers varying geographics, document types the entity accepts for eIDVT biometric matching, and individuals of diverse age, gender, and ethnicity demographics;

(b) only document fraud instruments that are reproduced forms of genuine documents (ie, printed versions of second-generation documents);

(c) no physically tampered documents;

(d) at least 30% document fraud instruments at level A representing at least 3 or more document fraud instrument species;

(e) at least 30% document fraud instruments at Level B representing at least 3 or more document fraud instrument species; and

(f) no document types that are considered out-of-scope for processing through the eIDVT.

Document verification transactions with physical document fraud instruments

(7) The biometric testing entity must perform testing with physical document fraud instruments according to the rules for transactions for testing for genuine physical documents as set out in section 7.3.1 of FIDO document authenticity verification requirements.

Metrics to be calculated for physical document fraud instruments

(8) The document false accept rate must be calculated in accordance with section 3.1.2 of FIDO document authenticity verification requirements.

(9) For physical testing with document fraud instruments, the entity's eIDVT biometric matching must achieve a document false reject rate of 1% or less.

5.32 Testing requirements for eIDVT

(1) In this rule:

optical character recognition or ***OCR*** means the process described in subrule 5.32(7).

(2) If an entity conducts eIDVT biometric matching in accordance with rule 5.24, the entity must ensure its biometric matching algorithm is tested by a biometric testing entity in accordance with this rule.

(3) The ISP's eIDVT must be tested according to, and meet the requirements of, the FIDO document authenticity verification requirements subject to the following amendments:

(a) the test sets for digital document testing as described in section 6.2 (test sets), must be reasonably balanced across document types and contain at least 30 of each listed document type supported by the eIDVT;

(b) the test set for physical document testing as described in section 7.2.2 (test crew and associated genuine documents) should be reasonably balanced across document types and must contain at least 10 of each listed document supported by the eIDVT; and

(c) the eIDVT must meet the criteria as described in 3.1 (performance levels) but must achieve a document false reject rate of 1% or below and the document false accept rate of 1%.

(4) The ISP must provide the Digital ID Regulator with a report from the biometric testing entity confirming that the entity's eIDVT has been tested in accordance with the FIDO document authenticity verification requirements and this rule.

(5) An entity must provide the Digital ID Regulator with a list of the types of credential that are accepted by the eIDVT for verification. A unique type of credential considers the following:

(a) kind of credential (for example, driver's licence or passport);

(b) issuer of credential; and

(c) series or version of credential.

(6) Where a new unique type of credential is included in an entity's eIDVT for verification, the entity must retest its eIDVT in accordance with the requirements in FIDO document authenticity verification requirements and this rule.

(7) An entity's eIDVT must:

(a) use optical character recognition (***OCR***) to convert an image of an acquired 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.

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

Subdivision 4—User experience

5.33 User experience requirements

(1) The ISP must provide individuals with a clear and simple description of each step of the identity proofing process, including a description of what the individual needs to do in order to complete each step.

(2) The ISP must notify individuals of the technical requirements for using the ISP's technology information system.

Note: Examples of such technical requirements includes access to a mobile phone or webcam.

(3) The ISP must:

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

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

(c) notify individuals of the consequences to the individual if they do not provide one or more credential.

(4) If an authenticator such as a digital code is issued by the ISP to an individual as part of the identity proofing process, the ISP must provide clear advance notice to the individual of:

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

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

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

(5) The ISP must notify the individual of the outcome of the identity proofing process as follows:

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

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

(i) information and credentials that will be destroyed by the entity;

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

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

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

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

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

(iii) an option to either:

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

(B) not continue with the proofing process.

(6) If the individual elects to:

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

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

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

(ii) notify the individual of the information and credentials that are to be destroyed.

(7) The ISP must provide support to individuals who need assistance during the identity proofing process, including providing clear instructions on how the individual can update their personal information collected by the ISP as part of the identity proofing process.

Note: Examples of appropriate support included support through a shopfront, a call centre that is contactable by the national relay service and a text-based support such as an online chat window.

Subdivision 5—Requirements for alternative proofing processes

5.34 Interpretation

(1) In this Subdivision:

alternative proofing process means a proofing process conducted in accordance with rule 5.35.

exceptional use case means a situation where an individual, in relation to the credentials required for the IP level sought by the individual:

(a) does not possess the credentials; and

(b) is unable to obtain the credentials in a reasonable timeframe considering the circumstances as to why the individual is unable to obtain the credentials.

5.35 Alternative proofing processes for exceptional use cases

(1) The ISP may only perform alternative proofing processes if it is authorised to do by an accreditation condition.

(2) Before undertaking an alternative proofing process to provide reusable digital IDs for exceptional use cases, an ISP must:

(a) perform a risk assessment associated with implementing the alternative process;

(b) detail the controls and risk mitigation strategies to be implemented in response to the assessed risks; and

(c) receive confirmation from the Digital ID Regulator in the entity's accreditation conditions that the entity is accredited to perform the

alternative proofing process and assert that it is equivalent to a particular identity proofing level.

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

(a) acceptance of alternative types of credentials;

(b) verification of an individual's claimed identity with an individual who is a trusted referee and whose identity has been verified to an equal or greater identity proofing level than the level requested in the alternative proofing process;

(c) verification of an individual's claimed identity with a reputable organisation known to the individual for example, Aboriginal and Torres Strait Islander organisations may be able to verify, the identity of individuals if no other government record exists;

(d) reliance on the identity proofing processes of other organisations that have verified the identity of the individual to the relevant identity proofing level;

(e) an interview with the individual to assess the consistency and legitimacy of the individual's claims, and the validity of the claimed identity;

(f) alternative methods for individuals to provide attributes or credentials to the entity – for example alternative methods may include the provision of certified copies of credentials by trusted third parties instead of attending an in-person interview where an individual can demonstrate they live in a remote area; and

(g) providing support for individuals to obtain evidence which, without limitation, may include assisting an individual to register their birth.

Part 3—Accredited attribute service providers

Division 1—Requirements

5.36 Verifying and managing

(1) When verifying or managing attributes of an individual, an ASP must comply with this Division.

(2) When verifying an attribute of an individual, an ASP must ensure the attribute is:

(a) uniquely identifiable in respect of the individual;

(b) current; and

(c) sufficiently bound to the individual claiming the attribute in accordance with subrule (3).

(3) An ASP must:

(a) identify to the entities and individuals involved in the transaction the identity proofing level that is required for an individual to claim that attribute; and

(b) ensure the individual has been proofed to the identity proofing level identified in subrule (a) in accordance with the requirements of Division 3 of Part 2 of this Chapter.

(4) Where an ASP is verifying an attribute, the ASP must do so by either:

(a) source verification (see rule 5.14); or

(b) technical verification (see rule 5.15).

5.37 Attribute provenance

(1) An ASP must make available to relying parties using the ASP's accredited services the following kinds of information:

(a) the identity proofing level required to bind the attribute to the digital ID;

(b) the authentication level in rule 5.45 relevant to the attribute bound to the digital ID;

(c) when the attribute was last updated;

(d) how the attribute was verified; and

(e) if the attribute is self-asserted by the individual and not verified, those facts.

Division 2—Requirements for attributes bound to a reusable digital ID

(1) When verifying or managing attributes bound to a reusable digital ID, an ASP must comply with this Division.

5.38 Attribute management

(1) An ASP must:

(a) determine the authentication level required for an individual to gain access to, manage or request disclosure of the attribute the ASP verifies or manages; and

Note: The determination will take into account the risks associated with the access or use of the relevant attribute, with applicable controls and risk mitigation strategies to be included as part of the ASP's fraud control plan and system security plan.

(b) authenticate the individual to this level before the individual gains access to, manages or consents to the disclosure of that attribute.

5.39 Suspend use of an attribute

(1) If an individual requests the ASP to suspend use of the individual's attribute, the ASP must:

(a) confirm the legitimacy of a request from an individual before preventing the continued use of the individual's attribute;

(b) take reasonable steps to suspend use of that attribute for the period requested; and

(c) notify the relevant authoritative source.

Note: The controls in place to assist an accredited entity to confirm the legitimacy of the request must be addressed in the entity's fraud control plan—see rule 4.29.

(2) If an ASP suspends use of an individual's attribute at the direction of the Digital ID Regulator, the ASP must provide a process for the individual to reactivate the attribute in accordance with rule 5.42.

5.40 Management of a suspected digital ID fraud incident or cyber security incident

(1) Where the verification of, update to or use of an attribute is identified as a suspected digital ID fraud incident or a suspected cyber security incident, an ASP must verify that the attribute has not been compromised.

(2) If an ASP detects a suspected digital ID fraud incident or cyber security incident in relation to an attribute, the ASP must take reasonable steps to verify and confirm that the individual has effective control of their attribute.

(3) If an ASP has taken reasonable steps in accordance with (2), but has not been able to verify and confirm that the individual has effective control of their attribute, the ASP must suspend use of the attribute.

(4) To reactivate an attribute that has been suspended due to a digital ID fraud incident or cyber security incident, an accredited entity must follow the process set out at rule 5.42.

5.41 Management of a digital ID fraud incident or cyber security incident of a digital ID

(1) If an ASP detects a digital ID fraud incident or cyber security incident in relation to an individual's attribute, the ASP must prevent the continued use of that attribute.

(2) To reactivate an attribute that has been suspended due to a digital ID fraud incident or cyber security incident, an accredited entity must follow the process set out at rule 5.42.

5.42 Reactivation of an attribute

(1) To reactivate an attribute, an ASP must bind the individual to the attribute in accordance with rule 5.36.

(2) An ASP will not be required to reactivate an attribute where the ASP no longer retains the relevant information to comply with subrule (1).

Part 4—Authentication management

5.43 Interpretation

(1) In this Part:

AACAs—see subrule 5.65(6).

AE-compromise resistance means authentication protocols that do not require an accredited entity to persistently store secrets that could be used for authentication.

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

authentication protocol means a defined sequence of messages between an individual and an accredited entity authorised to provide authenticator services that establishes the individual's digital ID by demonstrating that the individual has possession and effective control of one or more valid authenticators.

authentication request means a request for authentication from:

(a) an individual to an accredited entity or relying party; or

(b) an accredited entity or relying party to another accredited entity or relying party.

look-up secret means a physical or electronic record that stores a set of secrets shared between an individual and the accredited entity authorised to provide an authenticator service.

memorised secret means a secret value chosen and memorised by the individual, such as a password or PIN.

MF OTP—see subrule 5.69(1).

MitM—see subrule 5.65(6).

multi-factor cryptographic device or ***MF crypto device*** means a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor.

Note: Although cryptographic devices contain software, they differ from cryptographic software authenticators in that all embedded software on the hardware device is under the effective control of the accredited entity providing authentication management or the issuer.

multi-factor cryptographic software or ***MF crypto software*** means a cryptographic key that is stored in some form of removable media or device that requires activation through a second authentication factor.

multi-factor one-time password device or ***MF OTP device*** means a device that generates OTPs as part of an authentication activity.

Note: This includes hardware devices and software-based OTP generators installed on devices such as mobile phones. The OTP is displayed on the device and input or transmitted by an individual, proving possession and effective control of the device.

one-time password (OTP) means a password that is changed each time it is required.

out-of-band device means a physical device that uses an alternative channel for transmitting information.

phishing resistance means authentication methods implemented by an accredited entity for preventing and addressing impersonation attacks.

PSTN means a public switched telephone network.

replay resistance means protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorised effect or gaining unauthorised access.

single-factor cryptographic device or ***SF crypto device*** means a hardware device that performs cryptographic operations using one or more protected cryptographic keys and authenticated by proving possession and effective control of the cryptographic key.

single-factor cryptographic software or ***SF crypto software*** means a cryptographic key that is stored in some form of soft media.

single-factor one-time password or SF OTP device means a device that generates and displays OTPs, including hardware devices, SMS or software-based OTP generators installed on devices such as mobile phones.

Division 1—Preliminary

5.44 Application

(1) This Part applies to an accredited entity that provides authentication management.

Division 2—Requirements when accredited entity is providing authentication management

5.45 Authentication levels

(1) An accredited entity must not assert an authentication level for an authentication event unless each of the requirements in Table 2 for that authentication level has been met.

Note: A reference to ‘must’ in Table 2 means the requirement is mandatory.

Table 2: Authentication levels

Item	Requirement	AL1	AL2	AL3
1	Authenticator types	One of the following: (a) memorised secret; (b) look-up secret; (c) out-of-band device; (d) SF OTP device; (e) SF crypto software; (f) SF crypto device; (g) MF OTP device; (h) MF crypto software; (i) MF crypto device.	One of the following: (a) MF OTP device; (b) MF crypto software; (c) MF crypto device; or, a memorised secret and one the following: (d) look-up secret; (e) out-of-band device; (f) SF OTP device; (g) SF crypto software; (h) SF crypto device.	(a) MF crypto device; or (b) SF crypto device and memorised secret; or (c) SF OTP device and MF crypto software; or (d) SF OTP device and MF crypto device; or (e) SF OTP device and SF crypto software and memorised secret.
2	Reauthentication requirements	30 days	12 hours or 30 minutes of inactivity—must use at least 1 authentication factor.	12 hours or 15 minutes of inactivity—must use both authentication factors.
	Security requirements			
3	MitM resistance	Must	Must	Must
4	Phishing resistance	—	—	Must
5	AE-compromise resistance	—	—	Must
6	Replay resistance	—	Must	Must
7	Authentication intent	—	May	Must
8	Approved identity proofing combinations	IP1	IP1 to IP3 (inclusive)	All identity proofing levels

5.46 General requirements for authentication

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

(2) Before authenticating the digital ID of, or information about, individuals, an accredited entity must ensure that authenticators presented by an individual have not expired or been revoked.

(3) If an individual requests the accredited entity to suspend or deactivate the individual's authenticator, the accredited entity must:

(a) confirm the legitimacy of the request; and

(b) as soon as practicable after confirming the legitimacy of the request:

(i) suspend the use of the authenticator for the period requested; or

(ii) deactivate the authenticator.

5.47 Restricting the use of an authenticator

(1) If an accredited entity determines that the use or potential use of a kind of authenticator is resulting in or would result in an unacceptable risk to any individual, the entity must, as soon as practicable:

(a) prevent further use of that authenticator;

(b) notify affected individual using that kind of authenticator of the security risks;

(c) offer affected individual at least one alternative authenticator that can be used to authenticate at the required authenticator level; and

(d) address any additional risks to individuals in its system security plan in accordance with rule 4.10.

5.48 Physical authenticators

(1) For the purposes of this rule, a physical authenticator includes the following authenticators:

(a) look-up secrets;

(b) out-of-band devices;

(c) single-factor OTP device;

(d) multi-factor OTP device;

(e) single-factor cryptographic software;

(f) multi-factor OTP device;

(g) single-factor cryptographic device;

(h) multi-factor cryptographic software; and

(i) multi-factor cryptographic device.

(2) If an accredited entity conducts authentication using a physical authenticator, the entity must:

(a) provide individuals with clear instructions on how to protect the physical authenticator against theft or loss; and

(b) have a mechanism to immediately revoke or suspend the use of the authenticator if an individual notifies the entity of an actual or suspected loss or theft of the physical authenticator.

5.49 Compromised authenticator

(1) In this rule:

compromised authenticator means an authenticator that has been reported to, or identified by, the accredited entity as having been lost, stolen, damaged or duplicated without authorisation.

(2) If an accredited entity becomes aware that an authenticator is compromised, the entity must promptly suspend the use of, revoke or destroy the compromised authenticator.

(3) To facilitate secure reporting of a compromised authenticator, an accredited entity may provide affected individuals with a method of authenticating themselves to the entity using a backup or alternative authenticator.

(4) The backup or alternative authenticator referred to in subrule (3) must be either a memorised secret or a physical authenticator.

(5) If an accredited entity is informed that an authenticator has been compromised, it:

(a) may choose to validate an individual's contact details such as an email or mobile phone number; and

(b) must suspend the use of a compromised authenticator.

(6) An accredited entity may set a time limit after which the suspended authenticator can no longer be reactivated.

5.50 Expiry of an authenticator

(1) If an authenticator has expired, an accredited entity must not use that authenticator for authentication.

(2) As soon as practical after expiry of an authenticator or receipt by the individual of a renewed authenticator, an accredited entity must require the individual to surrender or prove destruction of any physical authenticator containing attribute certificates signed by the entity.

5.51 Revocation and termination of an authenticator

(1) An accredited entity must promptly revoke the binding of an authenticator when:

(a) an individual's digital ID associated with that authenticator ceases to exist;

(b) requested by the individual; or

(c) the entity determines that the individual no longer meets the entity's eligibility requirements.

Note: An account may cease to exist on the death of the individual or discovery that the account is fraudulent.

(2) An accredited entity must require an individual to surrender or prove destruction of any physical authenticator containing attribute certificates signed by the entity as soon as practical after revocation of the relevant certificate or termination of the individual's authenticator.

5.52 User experience requirements for authentication management

(1) An accredited entity providing authentication management must provide individuals with information about the use and maintenance of their authenticator, including:

(a) instructions on how to use the authenticator;

(b) when the authenticator will expire; and

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

5.53 System security plan

Out-of-band devices

(1) If an accredited entity conducts authentication using out-of-band devices, the entity must detail in its system security plan:

(a) the risks of using a PSTN as referred to in rule 5.67(14); and

(b) how those risks will be managed.

(2) the ISP must conduct the authentication using out-of-band devices in accordance with the risk-management strategies in its system security plan.

Division 3—Binding authenticators to a reusable digital ID

5.54 Authenticator binding

(1) An accredited entity must bind an authenticator to a digital ID by either:

(a) issuing the authenticator to the individual during the enrolment of the individual into the entity's DI data environment; or

(b) binding an acceptable authenticator provided by an individual to that digital ID.

(2) An accredited entity must maintain a record of all authenticators that are or have been bound to each digital ID within the entity's DI data environment.

(3) The record created by the entity for each authenticator must:

(a) contain information required to implement and support rate limiting required for rule 5.74;

(b) contain the date and time the authenticator was bound to the digital ID, and the relevant account number or identifier;

(c) include information about the source of the binding of any device associated with the enrolment; and

(d) contain information about the source of unsuccessful authentications attempted with the authenticator.

Note: For the purpose of subrule (c), examples of information include IP address and device identifier.

(4) When any new authenticator is bound to an individual's digital ID, an accredited entity must ensure that the binding protocol and the protocol for provisioning the associated cryptographic keys are done at a level of security commensurate with the authentication level at which the authenticator will be used.

5.55 Binding at enrolment

(1) For remote transactions where enrolment and binding cannot be completed in a single electronic transaction that is a single protected session, an accredited entity must ensure that:

(a) individuals identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction or sent to the individual's mobile phone number or email address; and

(b) long-term authentication secrets are only issued to an individual within a protected session.

(2) For in-person transactions where enrolment and binding cannot be completed in a single physical encounter within a single protected session, the accredited entity must ensure that:

(a) individuals identify themselves in-person by either presenting a secret as described in subrule (1)(a), or through use of biometric authentication in accordance with Division 4 of this Chapter;

(b) temporary secrets are not reused; and

(c) if the entity issues long-term authentication secrets during an in-person transaction, such secrets must be loaded locally onto a physical device that is issued in-person to the individual or delivered in a manner that confirms the individual's email address or mobile phone number.

5.56 Requirements for binding additional authenticators

(1) If an accredited entity binds additional authenticators to an individual's digital ID, the entity must comply with this rule.

(2) Before binding an additional authenticator to a digital ID, the entity must first require the individual to authenticate at the authentication level at which the new authenticator will be used, or a higher authentication level.

5.57 Renewal

(1) If the accredited entity issues authenticators that expire, the entity must bind an updated authenticator in a reasonable amount of time before the authenticator expires.

When the individual authenticates the individual's digital ID using the new authenticator, the entity must immediately revoke the authenticator it is replacing.

5.58 Step-up of an authentication level

(1) An accredited entity may allow an individual to step up the authentication level as a result of an authentication event to a higher authentication level in accordance with this rule.

(2) Before starting the authentication step-up process, the entity must first authenticate the individual's existing authenticator bound to the individual's digital ID.

(3) When an authenticator is bound to a digital ID as a result of a step-up process, the entity must ensure the new authenticator:

(a) meets all the requirements for the higher authentication level as set out in Table 2 of rule 5.45; and

(b) is of a type that compatible with the entity's information technology system.

Division 4—Requirements for biometric authentication

5.59 Interpretation

(1) In this Division:

authenticated protected channel means a communication channel that uses approved cryptography where the client connection has authenticated to the relevant server.

5.60 Application

(1) This Division applies to an accredited entity that is authorised by an accreditation condition to collect, use or disclose biometric information when providing an authenticator service.

5.61 Biometrics for authentication use

(1) For authentication, biometric information must only be used as a factor to unlock a multi-factor authenticator where the relevant authenticator:

(a) requires two or more factors to execute a single authentication event; and

(b) is possession-based, where the device is authenticated as a part of the single authentication event.

(2) An accredited entity may use biometric information for authentication using:

(a) in-device biometric capability in accordance with rule 5.62; or

(b) custom biometric capability in accordance with rule 5.63.

5.62 In-device biometric capability

(1) In this rule:

in-device capability means the built-in biometric capability provided by original equipment manufacturers for smartphones, including the biometric sensor, the presentation attack detection subsystem, and the biometric matching algorithm.

Note: Capabilities provided by online equipment manufacturers for smartphones include, for example, FaceID.

(2) An accredited entity:

(a) must only use in-device biometric capability as a factor for authentication events to meet AL1 or AL2; and

(b) must not use in-device biometric capability as a factor for AL3 authentication events.

(3) An accredited entity must ensure that the individual's device and in-device biometric capability are genuine when interacting with the entity's information technology system.

Note: This could be achieved by, but is not limited to performing authentication of the biometric sensor or endpoint, or performing runtime interrogation of signed metadata (e.g. attestation).

(4) An accredited entity must address risks, threats and vulnerabilities specific to the use of in-device capability in its fraud control plan, including, but not limited to risks, threats and vulnerabilities related to:

(a) biometrics associated with multiple individuals being enrolled on a single device;

(b) compromised devices and the effect this may have on the use of in-device biometric capability;

(c) the ability of individuals to adjust settings on their device relating to the security and performance of the device's biometric security settings; and

(d) vulnerabilities of in-device biometric capability that are publicly reported and not yet addressed by security patches for the device.

(5) An accredited entity must not allow the use of in-device biometric capability for its information technology system that operate on devices that cannot receive operating system security updates.

5.63 Custom biometric capability

(1) An accredited entity must ensure that an authenticated protected channel between the sensor and the accredited entity's information technology system is set up before capturing the biometric sample from the individual.

(2) An accredited entity must use a biometric matching algorithm to perform one-to-one biometric matching between the acquired biometric and the reference biometric.

(3) An accredited entity must perform the biometric matching using the biometric matching algorithm:

(a) locally on the individual's device; or

(b) centrally, being where the biometric information is transferred to the entity's information technology system and the biometric matching is performed remotely by the entity from the individual's device.

(4) If an accredited entity performs the biometric matching in accordance with subrule (3)(b):

(a) use of the biometric as an authentication factor must be limited to one or more specific devices that are identified using approved cryptography;

(b) a separate cryptographic key must be used for identifying the device, as distinct from the biometric factor;

(c) all transmission of biometrics must occur over the authenticated protected channel; and

(d) biometric template protection as per the requirements in ISO/IEC 24745 must be implemented.

(5) An accredited entity must test its biometric matching algorithm in accordance with rule 5.29, with the following exceptions:

(a) for accredited entities using biometric authentication for AL1 only, the accredited entity does not require a biometric testing entity to conduct the testing.

(6) An accredited entity must employ presentation attack detection based on data captured by both the data capture subsystem and through system level monitoring, as described by ISO 30107-1.

(7) An accredited entity must include liveness detection as part of presentation attack detection.

(8) An accredited entity must complete the capture of the acquired biometric and presentation attack detection processes as part of the same process before submission of the acquired biometric for biometric matching.

(9) An accredited entity must make the presentation attack detection decision either:

(a) locally on the individual's device; or

(b) centrally being where the biometric information is transferred to the entity's information technology system and the biometric matching is performed remotely by the entity from the individual's device.

(10) An accredited entity's presentation attack detection must allow no more than 5 consecutive failed authentication attempts.

(11) Once the limit of consecutive failed attempts has been reached, the custom biometric capability must either:

(a) impose a delay of at least 30 seconds before the individual's next attempt to authenticate using custom biometric capability, increasing exponentially with each successive attempt (e.g., 1 minute before the following attempt, 2 minutes before the second following attempt); or

(b) disable the custom biometric capability for authentication and offer another authentication factor (i.e., a different biometric modality or a PIN/passcode if not already a required factor) .

(12) An accredited entity must test its biometric matching algorithm in accordance with rule 5.28, with the following exceptions:

(a) For rule 5.28(6) —all presentation attack instrument species used in testing must have an attack presentation classification error rate (APCER) of no more than 10%.

(b) For accredited entities using biometric authentication for AL1 only, the accredited entity does not require a biometric testing entity to conduct the testing.

Division 5—Data standards for authentication management

Subdivision 1—Kinds of authenticators

5.64 General

(1) An accredited entity must comply with the requirements in this Division, for each kind of authenticator specified in Table 2 in this Chapter.

5.65 Memorised secrets

(1) If an accredited entity provides memorised secrets, it must comply with this rule.

(2) Memorised secrets chosen by the individual must be at least 8 characters long.

(3) Memorised secrets chosen randomly by the entity must be at least 6 characters in length and may be entirely numeric.

(4) When processing requests from an individual to establish or change a memorised secret, the entity must compare the prospective secret against a list that contains secrets known to be commonly used, expected or compromised.

Note: The list for subrule (4) may include:

(a) passwords obtained from previous breach corpuses;

(b) dictionary words;

(c) repetitive or sequential characters (e.g. “aaaaaa”, “1234abcd”); and

(d) context-specific words, such as the name of the service, the username, and derivatives thereof.

(5) If the chosen secret is found in the list, the entity must:

(a) notify the individual that they need to select a different secret;

(b) provide the reason for rejection; and

(c) require the individual to choose a different secret.

(6) When requesting memorised secrets, an accredited entity’s information technology system must use Australian Signals Approved Cryptographic Algorithms (***AACAs***) and an authenticated protected channel.

(7) memorised secrets must be stored in a form that is resistant to offline attacks, including by ensuring:

(a) memorised secrets are salted and hashed using a suitable one-way cryptographic key derivation function;

(b) the salt value is at least 32 bits in length and be chosen arbitrarily so as to minimise salt value collisions among stored hashes; and

(c) both the salt value and the resulting hash are stored for each individual who uses memorised secrets.

5.66 Look-up secrets

(1) If an accredited entity provides look-up secrets, it must comply with this rule.

(2) Look-up secrets must be delivered to the individual in a secure manner.

(3) the individual must be prompted for the next secret from the individual’s authenticator or for a specific secret.

Note: The specific secret may be, for example, the next numbered secret.

(4) A look-up secret given to an individual must only be used successfully once.

(5) If the lookup secret is derived from a grid card, each cell of the grid must be used only once.

(6) An accredited entity must store look-up secrets in a form that is resistant to offline attacks, including by ensuring:

(a) look-up secrets are to be hashed using an AACA; and

(b) for look-up secrets that have more than 128 bits of entropy, the look-up secret is salted before being hashed with a salt value that is at least 32 bits in length and arbitrarily chosen so as to minimise salt value collisions among stored hashes.

(7) For each individual who uses look-up secrets, an accredited entity must store both the salt value and the resulting hash referred to in subrule (6)(b).

(8) For look-up secrets that have less than 64 bits of entropy, a rate-limiting mechanism must be implemented that effectively limits the number of failed authentication attempts that can be made on the individual's digital ID.

Note: Rate limiting mechanisms are addressed in rule 5.74.

(9) When requesting look-up secrets to provide resistance to eavesdropping and Man-in-the-Middle (***MitM***) attacks, an accredited entity must use AACAs and an authenticated protected channel.

5.67 Out-of-band devices

(1) If an accredited entity provides out-of-band devices, it must comply with this rule.

(2) The out-of-band device must establish a separate channel with an accredited entity's information technology system to retrieve the out-of-band secret or authentication request.

Note: This separate channel is out-of-band with respect to the primary communication channel (even if it terminates on the same device), provided the device does not leak information from one channel to the other without the consent of the individual.

(3) The out-of-band device must uniquely authenticate itself in one of the following ways when communicating with an accredited entity's information technology system:

(a) establish an authenticated protected channel to the entity's information technology system that:

(i) uses approved cryptography; and

(ii) stores relevant cryptographic keys in suitably secure storage available to the authenticator application; or

(b) only where a secret is being sent from the entity's information technology system to the out-of-band device via the PSTN, authenticate to a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device.

Note: Subrule (a): for example, keychain storage, secure element etc.

(4) If the out-of-band device sends an approval message over the secondary communication channel, rather than by the individual transferring a received secret to the primary communication channel, then:

(a) an accredited entity must ensure that either:

(i) the device accepts transfer of the secret from the primary channel, which secret must be sent to the entity's information technology system over the secondary channel to associate the approval with the authentication transaction; or

(ii) the device:

(A) presents a secret received via the secondary channel from the entity's information technology system;

(B) prompts the individual to verify the consistency of that secret with the primary channel, before accepting a yes/no response from the individual; and

(C) sends that response to the entity's information technology system.

Note: For subrule (a)(i): the individual may perform the transfer manually or use a technology such as a barcode or QR code to affect the transfer.

(5) If out-of-band verification is to be made using a secure application on a device, an accredited entity's information technology system may send a push notification to that device, in which case the entity's information technology system must wait for the establishment of an authenticated protected channel and verify the device's identifying cryptographic key.

(6) An accredited entity must not store the identifying cryptographic key received referred to in subrule (5).

(7) An accredited entity must ensure its information technology system:

(a) uses a verification method to uniquely identify the device; and

(b) authenticates the device before transmitting the authentication secret to the device.

(8) Depending on the type of out-of-band device, an accredited entity must ensure that the entity's information technology system:

(a) transfers the secret to the primary channel as follows:

(i) signal the device containing the individual's authenticator to indicate readiness to authenticate;

(ii) after transmitting such signal, transmit a random authentication secret to the out-of-band device; and

(iii) wait for the random authentication secret to be returned on the primary communication channel; or

(b) transfers the secret to the secondary channel as follows:

(i) display a random authentication secret to the individual via the primary channel; and

(ii) wait for the random authentication secret to be returned on the secondary channel from the individual's out-of-band device; or

(c) obtains verification of secrets from the individual as follows:

(i) displays a random authentication secret to the individual via the primary channel;

(ii) sends the same random authentication secret to the out-of-band device via the secondary channel for presentation to the individual; and

(iii) after transmitting the random authentication secret referred to in paragraphs (i) and (ii), waiting for an approval (or disapproval) message via the secondary channel.

(9) For each option referred to in subrule (8), the authentication must be considered invalid if each of the relevant actions are not completed within 10 minutes.

(10) To provide replay resistance, an accredited entity's information technology system must not accept a given authentication secret more than once during the validity period.

(11) An accredited entity must generate random authentication secrets with at least 20 bits of entropy.

(12) If the random authentication secret has less than 64 bits of entropy, an accredited entity must ensure its information technology system incorporates a rate-limiting mechanism that limits the number of failed authentication attempts that can be made on a digital ID.

Note: Rate limiting mechanisms are addressed in rule 5.74.

(13) If out-of-band verification is to be made using the PSTN, an accredited entity must verify that the pre-registered telephone number being used is associated with a specific physical device.

(14) An accredited entity must consider risks associated with device swap, SIM change, number porting or other abnormal behaviour before using the PSTN to deliver an out-of-band authentication secret.

5.68 Single-factor one-time password devices

(1) If an accredited entity provides SF OTP devices, the entity must comply with this rule.

(2) The secret cryptographic key and its algorithm must provide the minimum-security strength specified in the latest edition of the ISM.

(3) The nonce must be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

(4) OTP authenticators must not facilitate the cloning of the secret cryptographic key onto multiple devices.

(5) If the nonce used to generate the authentication output is based on a real-time clock, the nonce must be changed at least once every 2 minutes.

(6) The OTP value associated with a given nonce must not be accepted more than once.

(7) When a single-factor OTP authenticator is being associated with a digital ID, an accredited entity must use AACAs to either generate and exchange or to obtain the secrets required to duplicate the authentication output.

(8) An accredited entity must use AACAs and an authenticated protected channel when collecting the OTP to provide resistance to eavesdropping and MitM attacks.

(9) To provide replay resistance, an accredited entity's information technology system must not accept a given time-based OTP more than once during the validity period of such authenticator.

(10) Time-based OTPs must have a defined lifetime that is determined by the expected clock drift - in either direction - of the authenticator over its lifetime, plus allowance for network delay and individual entry of the OTP.

(11) If the authentication output has less than 64 bits of entropy, an accredited entity must ensure its information technology system incorporates a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on a digital ID.

Note: Rate limiting mechanisms are addressed in rule 5.74.

5.69 Multi-factor one-time password devices

(1) If an accredited entity provides multi-factor one-time password (**MF OTP**) devices, the entity must comply with this rule.

(2) The secret cryptographic key and its algorithm must provide at least the minimum-security strength specified in the latest edition of the ISM.

(3) The nonce must be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.

(4) OTP authentication must not facilitate the cloning of the secret cryptographic key onto multiple devices.

(5) If the nonce used to generate the authentication output is based on a real-time clock, the nonce must be changed at least once every 2 minutes.

(6) Any memorised secret used for activation must be a randomly chosen numeric secret at least 6 decimal digits in length.

(7) The unencrypted key and activation secret or biometric sample - and any biometric information derived from the biometric sample, such as a probe produced through signal processing - must be zeroised immediately after an OTP has been generated.

(8) When a MF OTP authenticator is being associated with a digital ID, an accredited entity must use AACAs to either generate and exchange, or to obtain the secrets required to duplicate the authentication output.

(9) An accredited entity must use AACAs and an authenticated protected channel when collecting the OTP to provide resistance to eavesdropping and MitM attacks.

(10) An accredited entity must also establish that the MF OTP authenticator is a MF OTP device.

(11) Time-based OTPs must have a defined lifetime that is determined by the expected clock drift - in either direction - of the authenticator over its lifetime, plus allowance for network delay and individual entry of the OTP.

(12) To provide replay resistance, an accredited entity's information technology system must not accept a given time-based OTP more than once during the validity period of the authenticator.

(13) If the authentication output has less than 64 bits of entropy, an accredited entity must ensure its information technology system incorporates a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made in respect of the individual's digital ID.

Note: Rate limiting mechanisms are addressed in rule 5.74 .

5.70 Single-factor cryptographic software

(1) If an accredited entity provides single-factor cryptographic software, the entity must comply with this rule.

(2) The cryptographic key must be protected against unauthorised disclosure using access controls that limit access to the key to only those software components on the device requiring access.

(3) Single-factor cryptographic software authenticators must not facilitate the cloning of the secret cryptographic key onto multiple devices.

(4) Cryptographic keys must be protected against modification.

(5) Cryptographic keys must be protected against unauthorised disclosure.

(6) The challenge nonce must be at least 64 bits in length.

(7) The challenge nonce must either be unique over the authenticator's lifetime or be statistically unique.

(8) The authentication event must use approved cryptography.

5.71 Single-factor cryptographic devices

(1) If an accredited entity provides single-factor cryptographic devices, the entity must comply with this rule.

(2) Single-factor cryptographic devices must encapsulate one or more secret cryptographic keys, unique to the device, that cannot be removed from the device.

(3) The secret cryptographic key and its algorithm must provide at least 112 bits of effective security strength.

(4) The challenge nonce must be at least 64 bits in length.

(5) The challenge nonce must either be unique over the authenticator's lifetime, or be statistically unique.

(6) Approved cryptography must be used for authentication events.

(7) Cryptographic keys must be protected against modification.

(8) Cryptographic keys must be protected against unauthorised disclosure.

5.72 Multi-factor cryptographic software

(1) If an accredited entity provides multi-factor cryptographic software, the entity must comply with this rule.

(2) Access controls that limit access to the cryptographic key to only those software components on the device requiring access must be used.

(3) Authentication events must require the input of both factors.

(4) Any memorised secret used for activation must be a randomly chosen numeric value at least 6 decimal digits in length.

(5) The unencrypted key, and activation secret or biometric sample, and any biometric information derived from the biometric sample (such as a probe produced through signal processing) must be zeroised immediately after an authentication has taken place.

(6) Cryptographic keys must be protected against modification.

(7) Cryptographic keys must be protected against unauthorised disclosure.

(8) The challenge nonce must be at least 64 bits in length.

(9) The challenge nonce must either be unique over the authenticator's lifetime or be statistically unique.

(10) The authentication event must use approved cryptography.

(11) Truncation must not be performed on the memorised secret used for activation.

5.73 Multi-factor cryptographic devices

(1) If an accredited entity provides multi-factor cryptographic devices, the entity must comply with this rule.

(2) The secret cryptographic key and its algorithm must provide at least the minimum-security strength specified in the latest edition of the ISM.

(3) The challenge nonce must be at least 64 bits in length.

(4) The challenge nonce must either be unique over the authenticator's lifetime, or be statistically unique.

(5) Approved cryptography must be used for authentication events.

(6) Cryptographic keys must be protected against modification.

(7) Cryptographic keys must be protected against unauthorised disclosure.

Subdivision 2—General data standards

5.74 Rate limiting (throttling)

(1) In relation to the authenticator types referred to in subrule(2), an accredited entity must:

(a) implement and maintain rate limiting (throttling) for all authenticators;

(b) implement and maintain controls for its information technology system to protect authenticators against online guessing attacks; and

(c) limit consecutive failed authentication attempts on a single digital ID account to no more than 100.

(2) Subrule (1) applies to the following authenticator types:

(a) memorised secret;

(b) look-up secret;

(c) out-of-band device;

(d) single-factor OTP; and

(e) multi-factor OTP.

5.75 Authenticator attestation

(1) If the accredited entity uses authenticator attestation and the authenticator attestation is signed, it must be signed using a digital signature that provides at least 112 bits of effective security strength.

5.76 Phishing resistance

(1) In this rule:

private key means the cryptographic key in an asymmetric cryptographic key pair that must be kept secret.

(2) For authentication level 3, the requirements of this rule apply.

(3) A phishing resistant authentication protocol must:

(a) establish an authenticated protected channel with the entity's information technology system; and

(b) strongly and irreversibly bind a channel identifier that was negotiated in establishing the authenticated protected channel to the authentication output.

Note: The binding may occur by signing the two values together using a private key controlled by the individual for which the public key is known to the entity.

(4) The ISP's information technology system must validate the signature or other information used to prove phishing resistance.

(5) An AACA must be used to establish phishing resistance.

(6) Cryptographic keys used in accordance with rule 4.21 for the purpose of establishing phishing resistance must provide at least 112 bits of effective security strength.

(7) Authenticators that involve the manual entry of an authentication output, such as out-of-band and OTP authenticators, are not phishing resistant.

5.77 ISP-authenticator communications

(1) Where the ISP and the entity providing authentication management have separate information technology systems, communication between the ISP and the other entity must occur through a mutually authenticated secure channel using approved cryptography.

Note: An example of a mutually authenticated secure channel is a client authenticated TLS connection.

5.78 AE-compromise resistance

(1) For authentication level 3, the following requirements apply:

(a) public keys stored by the entity must be associated with the use of AACAs; and

(b) cryptographic keys must provide at least 112 bits of effective security strength.

5.79 Authentication intent

(1) For authentication level 3, the following requirements apply:

(a) the authentication intent must be established by the authenticator itself.

(b) Without limiting this rule, authentication intent may be established by the authenticator through use of:

(i) authentication processes that require the individual's intervention—an example is the individual entering an authentication output from an OTP device; or

(ii) cryptographic devices that require an individual's action, such as pushing a button or reinsertion, for each authentication or reauthentication operation—an example is the individual pushing a button or reinserting the cryptographic device.

5.80 Reauthentication

(1) In this rule:

reauthentication means the process by which the accredited entity reconfirms that a session is still under the control of the individual.

(2) For reauthentication, the following requirements apply:

(a) continuity of authenticated sessions must be based on the possession of a session secret issued by the accredited entity at the time o authentication and optionally refreshed during the session;

(b) session secrets must be non-persistent;

(c) session secrets must not be retained across a restart of the associated application or a reboot of the host device;

(d) periodic reauthentication of sessions must be performed to confirm the continued physical presence of the individual at an authenticated session— see item 2 of Table 2 for reauthentication requirements; and

(e) when a session has been terminated the individual must be required to establish a new session by authenticating again at the applicable authentication level.

Part 5—Accredited identity exchange provider

Division 1—Requirements for IXPs

5.81 General

(1) Where an IXP is conveying, managing or facilitating the flow of information between parties in a digital ID system, it must comply with this Part.

(2) An IXP must securely identify and authenticate each individual, accredited entity, entity or relying party involved in a transaction before conveying, managing or facilitating the flow of information between each party in that digital ID system.

5.82 Single sign on

(1) If an IXP provides single sign on, the IXP must:

(a) allow a relying party to request that an individual authenticates regardless of whether a pre-existing session exists; and

(b) implement a single logout mechanism.

(2) For a single sign on, an IXP may securely cache attributes obtained from an ISP or ASP for the duration of an authenticated session.

(3) If an IXP securely caches attributes referred to in subrule (2), such attributes must not be accessible to the IXP's personnel.

5.83 Digital ID system rules

(1) This rule applies to an IXP operating in a digital ID system:

(a) other than the Australian Government Digital ID System; and

(b) where one of more identity service providers participating in that system is not an accredited identity service provider.

(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 identity service providers participating in the system that are not accredited;

(b) are enforceable to the extent that the IXP, or another person able to enforce the system rules, can revoke the identity service provider's participation in the system for non-compliance with the system rules; and

(c) are not inconsistent with the Act and these rules.

(d) require that all information conveyed or managed within the system is dealt with in accordance with approved cryptography as if required by rule 4.19 applied to the identity service provider;

(e) require that an identity service provider participating in the system must not:

(i) disclose an attribute of an individual without the express consent of the individual;

(ii) collect, use, hold or disclose biometric information of an individual without the express consent of the individual;

(f) provide detail on how the identity service provider can collect, use, hold and disclose biometric information of an individual; and

(g) prohibit one-to-many biometric matching of an individual.

5.84 Annual transparency report

(1) At least once in each 12-month period after the IXP's accreditation day, the IXP must publish, in an open and accessible manner, an annual transparency report that details requests by an enforcement body for access to digital ID information held by the IXP.

(2) Subrule (1) does not apply if, in the 12-month period, the IXP has not received any such requests.

(3) Unless prohibited by law, an annual transparency report must include the following information:

(a) the name of each enforcement body that requested digital ID information from the IXP since the previous report;

(b) the total number of requests to the IXP by each enforcement body since the previous report;

(c) details of the kind of digital ID information requested by each enforcement body, but not so as to include personal information of an individual; and

(d) the total number of requests from each enforcement body that resulted in the entity providing digital ID information in response to the request.

Chapter 6 Annual reviews

Part 1—Requirements

6.1 General

(1) On or before the 12-month anniversary of the entity's accreditation day each year, an accredited entity must conduct an annual review in accordance with this Chapter and prepare an annual review report in accordance with Part 2 of this Chapter.

(2) Assurance assessments, systems testing and other testing conducted for an annual review must be conducted as close as practical to the end of the relevant 12-month period.

6.2 Scope of annual review

Review of changes

(1) An accredited entity must identify and record all changes to the entity's DI data environment, accredited services and statement of scope and applicability:

(a) since its accreditation day, in the case of the entity's first annual review; or

(b) otherwise, any changes that were not recorded in the prior annual review report.

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

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

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

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

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

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

each such change being a material change (***material change***).

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

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

requird to ensure the entity continues to comply with the controls and requirements reviewed and assessed;

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

(b) technical testing that complies with the requirements specified in paragraphs 2.4(1)(a) to (e) to the extent that each of those requirements relates to the material change, and prepare a report of the testing that complies with the requirements subrule 2.4(2);

(c) presentation attack detection testing that complies with the requirements of rule 5.28 to the extent that those requirements relate to the material change; and

(d) for an accredited identity service provider that conducts biometric binding, or biometric authentication in accordance with the applicable type of biometric testing in rules 5.26 to 5.32 that the material change affects.

DI data environment

(4) The accredited entity must review the boundaries of its DI data environment, and must do so in accordance with rule 2.6 as if the references in that rule to 'applicant' were to the 'accredited entity'.

Review of statement of scope and applicability

(5) The accredited entity must review its statement of scope and applicability for completeness and accuracy:

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

(b) where no such material changes occur—at least annually.

Review of assurance assessments and systems testing

(6) Where the accredited entity's response to an assessor's report of an assurance assessment or systems testing, provides a timeframe for the entity to implement any treatment for an identified risk or any recommendation, the accredited entity must provide in its annual review report details of the:

(a) treatment undertaken;

(b) implementation of the recommendation; and

(c) when the treatment or implementation occurred, or will occur.

(7) Subrule (6) applies to any assessor's report, including for a prior 12-month period, where the treatment or recommendation specified in that report will not be implemented by the time the entity provides its annual review report for the 12-month period under review.

6.3 Assurance assessments

Fraud assessment

(1) For every second annual review commencing on the accredited entity's accreditation day, the entity must conduct a fraud assessment.

(2) Despite subrule 3.7(2), the fraud assessment may be conducted by an assessor who does not meet the additional requirements in that rule if:

(a) in the previous two years, a fraud assessment has been conducted by assessor who meets the requirements in subrule 3.7(2); and

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

Protective security assessment

(3) For every second annual review commencing on the accredited entity's accreditation day, the entity must complete a protective security assessment.

6.4 Testing

Presentation attack detection testing

(1) For every second annual review commencing on the accredited entity's accreditation day, the entity must conduct presentation attack detection testing in accordance with rule 5.28.

Note: This rule is limited to accredited entities who provide biometric binding or biometric authentication, and then only to the extent the testing is relevant to the kind of biometric binding or biometric authentication provided by the accredited entity – see rule 2.2(1)(n).

Penetration testing

(2) For each annual review, an accredited entity must conduct penetration testing and respond to the testing report, each in accordance with the requirements set out in Division 1 of Part 3 of Chapter 3.

Part 2—Annual review report

6.5 Content of report

(1) For each annual review, the accredited entity must provide to the Digital ID Regulator on or before the end of the 12-month period under review, a report that contains the information and documents required by this Part.

6.6 Attestation statement

(1) The report must include an attestation statement, signed by the accredited entity's accountable executive, that attests that in the relevant 12-month period:

(a) the entity has reviewed changes in accordance with rule 6.2 and correctly identified material changes (as referred to in subrule 6.2(2));

(b) the entity has reviewed:

(i) system security plan;

(ii) fraud control plan;

(iii) disaster recovery and business continuity plan;

(iv) privacy policy;

(v) privacy management plan; and

(vi) data breach response plan; and

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

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

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

6.7 Information and documents

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

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

(c) a copy of the accredited entity's cyber security risk assessment (see rule 4.5);

(d) a copy of the accredited entity's fraud risk assessment (see rule 4.23);

(e) for accredited entities participating in any digital ID system other than the Australian Government Digital ID System:

(i) the number (including nil) of digital ID fraud incidents and cyber security incidents that occurred; and

(ii) where there has been an incident:

(A) the date of the incident;

(B) a description of each type of incidents and its severity; and

(C) a description of the measures taken by the entity in response to the incidents covered by the report; and

(f) a copy of any privacy impact assessments involving the accredited entity's DI data environment or accredited services and a copy of the entity's response to the assessment;

(g) the results of the biometric testing (see rule 4.43(6));

(h) for an accredited identity service provider that conducts biometric binding, or biometric authentication in accordance with the applicable type of biometric testing:

(i) the results of the entity's testing of its biometric matching algorithm (see rule 5.29(5));

(ii) the results of the entity's eIDVT testing (see rule 5.32(4)); and

(iii) evidence that the entity has completed source biometric matching testing (see rule 5.30); and

(i) for an accredited identity exchange provider, a copy, or link to, its annual transparency report.

Schedule 1 Credential requirements

Exposure Draft Note: the structure and presentation of this schedule is being reviewed to clarify the credential combinations and verification requirements.

Table 1 – COI credentials

Item	Credential type	Credential requirements	Verification requirements
1	Australian birth certificate	Issued by an Australian State or Territory Government Register of Births, Deaths and Marriages.	Source Visual
2	Australian passport	Issued in the individual's name or former name, within 3 years of the expiry date.	Source Visual
3	Australian ePassport	Issued in the individual's name or former name, within 3 years of the expiry date.	Source Technical Visual
4	Australian citizenship certificate	Issued in the individual's name or former name. If the individual's name appears on the Australian citizenship certificate of their parent, the individual may use that certificate.	Source Visual
5	Certificate of Registration by Descent	Issued in the individual's name or former name by the Australian Government as verification of the individual's Australian citizenship.	Source Visual
6	Australian Visa	Issued in the individual's name and attached to a current passport issued by a foreign country.	Source
7	DFAT issued Certificate of Identity	Issued in the individual's name or former name by the Department of Foreign Affairs and Trade.	Source Visual
8	DFAT issued Document of Identity	Issued in the individual's name or former name by the Department of Foreign Affairs and Trade.	Source Visual
9	UN Convention Travel Document (*Titre de Voyage*)	Issued in the individual's name or former name by the Department of Foreign Affairs and Trade	Source Visual
10	ImmiCard	A card issued in the individual's name or former name by the Department of Home Affairs.	Source Visual
11	Aboriginal and/or Torres	This includes proof of Aboriginal and/or Torres Strait Islander heritage.	Visual

Item	Credential type	Credential requirements	Verification requirements
	Strait Islander descent records		

Note: For the purposes of item 2 and 3 of the above table, an Australian Passport and Australian ePassport can be used as a COI credential for up to level IP3. Australian Passports must not be accepted as a COI credential for identity proofing to the level IP4.

Table 2 – Linking credentials

Item	Credential name	Credential requirements	Verification requirements
1	Australian marriage certificate	Issued by an Australian State or Territory Government.	Source Visual
2	Change of name certificate	Legal change of name or deed poll certificate.	Source Visual
3	Australian divorce papers	In the individual's name or former name. For example, a decree nisi or decree absolute.	Visual
4	Commonwealth victims' certificate	Issued by a magistrate in an Australian State or Territory.	Visual
5	Australian birth certificate	Issued by a State or Territory Government Register of Births, Deaths and Marriages.	Source Visual

Table 3 – UiTC credentials

Item	Credential name	Credential requirements	Verification requirements
1	Concession and Health Care Cards	Issued by Services Australia.	Source Visual
2	Medicare Card	Issued by Services Australia.	Source Visual
3	Student ID card	A current student ID card issued by an Australian secondary school, TAFE, university or registered training organisation. The card must include the individual's name or former name.	Visual
4	Bank or financial institution card, passbook, statement	Issued by a bank, credit union or building society. Statements or passbooks must cover at least 6 months of financial transactions and be in the individual's name. The individual's signature must be on the card and the individual's current address must be on the statement or passbook.	Source Visual

Item	Credential name	Credential requirements	Verification requirements
		A credential from a foreign bank or institution is not acceptable.	
5	Education certificate or certified academic transcript	Issued by an Australian secondary school, TAFE, university or registered training organisation. The transcript must include the individual's name or former name.	Source Visual
6	Mortgage papers	For an Australian property in the individual's name or former name. Prepared by an Australian legal practitioner.	Visual.
7	Veterans Affairs card	A current card issued in the individual's name by the Department of Veterans' Affairs.	Visual
8	Tenancy agreement or lease	An agreement or lease to which the individual is a party, showing the individual's current address.	Visual
9	Motor vehicle registration	Current registration papers with the individual's name, address and proof of payment.	Source Visual
10	Rates notice	A paid rates notice less than 12 months old issued in the individual's name, showing the individual's current address.	Visual
11	Electoral enrolment	Proof of the individual's enrolment in an electoral role maintained under law, showing the individual's current address.	Source Visual
12	Postal records	A history of at least 6 months of postal deliveries.	Source Visual
13	Telephone records	Records showing at least 6 months of phone usage.	Source Visual
14	Any credentials listed in the photo ID category	If not used elsewhere.	Source Technical Visual
15	Utility account	Issued in the individual's name, showing the individual's current address. The credential must be less than 6 months old.	Visual
16	Superannuation statement	Issued in the individual's name, showing the individual's current address. The credential must be less than 6 months old.	Visual
17	Senior's card	Issued in the individual's name.	Visual
18	Land titles office records	Issued in the individual's name.	Visual

Item	Credential name	Credential requirements	Verification requirements
19	Insurance policy renewal	Current insurance renewal for house and contents, vehicle or boat, or similar insurance, where the individual is the insured and the applicable policy has been held for over 12 months.	Source Visual

Table 4 – Photo ID

Item	Credential name	Credential requirements	Verification requirements
1	Australian passport	Issued in the individual's name or former name, within 3 years of the expiry date.	Source Visual
2	Australian ePassport	Issued in the individual's name or former name, within 3 years of the expiry date.	Source Technical Visual
3	Australian State or Territory issued drivers licence (includes a digital drivers licence)	A licence issued by an Australian State or Territory Government in the individual's name with the individual's photo. For digital drivers' licence, the security features must be tested to ensure authenticity.	Source Technical Visual
4	Foreign passport	A passport issued by another country, with a Source Verified valid entry stamp or Australian Visa, where applicable.	Visual Technical Visual
5	Foreign ePassport	A passport issued by another country, with a Source Verified valid entry stamp or Australian Visa, where applicable.	Technical Visual
6	Foreign military or defence force ID card	An identification card issued in the name of an individual by a foreign government showing a picture of the individual and identifying the individual as a current member of the military or defence forces of that government	Visual
7	Titre de Voyage / DFAT issued UN Convention travel documents	Issued in the individual's name or former name by the Department of Foreign Affairs and Trade.	Source Visual
8	Australian citizenship certificate	Issued in the individual's name or former name by the Department of Home Affairs.	Source
9	Indigenous community card	A card used to provide confirmation of identity for Aboriginal or Torres Strait Islanders who have not provided other credentials.	Visual

Item	Credential name	Credential requirements	Verification requirements
10	Shooter or firearms licence	A current card issued in the individual's name and including a photo of the individuals.	Visual
11	Aviation security identity card	A current card issued in the individual's name and including a photo of the individual.	Visual Source
12	Maritime security identity card	A current card issued in the individual's name and including a photo of the individual.	Visual Source
13	Australian Government issued photo ID card (employee ID)	A current card issued by the Commonwealth, or an Australian State or Territory Government, in the individual's name and including a photo of the individual.	Visual
14	Australian Department of Defence Highly Trusted Token	A current card issued in the individual's name and including a photo of the individual	Technical Visual
15	Defence Force identity card	Issued by the Australian Defence Force, and including the name and a photo of the individual.	Visual
16	Police identity card	A current card issued in the individual's name and including a photo of the individual.	Visual
17	Australian State or Territory issued trade (work or business) licence	A current card issued in the individual's name and including a photo of the individual (e.g. trade licences, real estate agents, security agents etc.)	Visual
18	Tangentyere ID card	Issued by the Tangentyere Council Aboriginal Corporation, and including the individual's name and a photo of the individual.	Visual
19	Proof-of-age card	Issued by an Australian State or Territory Government in the individual's name and including a photo of the individual.	Visual
20	Australia Post Keypass	A current card issued in the individual's name and including a photo of the individual.	Source Visual
21	Working with children / vulnerable people card	A current card issued in the individual's name and including a photo of the individual.	Source Visual

Note: A foreign passport can be used to satisfy the requirement in Table 3 for a UiTC credential if it has not already been provided as part of the Australian Visa for a COI credential (see item 6 of Table 1 of this Schedule).

Schedule 2 PSPF requirement list

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 1	B.1		The accountable authority of each entity must:	a. determine their entity's tolerance for security risks
PSPF Policy 1	B.1			b. manage the security risks of their entity, and
PSPF Policy 1	B.1			c. consider the implications their risk management decisions have for other entities, and share information on risks where appropriate.
PSPF Policy 2	B.1		The accountable authority must:	a. appoint a Chief Security Officer (CSO) at the Senior Executive Service1 level to be responsible for security in the entity
PSPF Policy 2	B.1			b. empower the CSO to make decisions about: i. appointing security advisors within the entity ii. the entity's protective security planning iii. the entity's protective security practices and procedures iv. investigating, responding to, and reporting on security incidents
PSPF Policy 2	B.1			c. ensure personnel and contractors are aware of their collective responsibility to foster a positive

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
				security culture, and are provided sufficient information and training to support this
PSPF Policy 2		Requirement 1. Security advisors	The CSO must be responsible for directing all areas of security to protect the entity's people, information (including ICT) and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.	
PSPF Policy 2		Requirement 2. Security procedures	Entities must develop and use procedures that ensure:	a. all elements of the entity's security plan are achieved
PSPF Policy 2		Requirement 2. Security procedures		b. security incidents are investigated, responded to, and reported
PSPF Policy 2		Requirement 2. Security procedures		c. relevant security policy or legislative obligations are met.
PSPF Policy 2		Requirement 3. Security training	Entities must provide all personnel, including contractors, with security awareness training at engagement and annually thereafter.	
PSPF Policy 2		Requirement 4. Specific training	Entities must provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training targeted to the scope and nature of the position.	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 2		Requirement 5. General email[1]	Entities must maintain a monitored email address as the central conduit for all security-related matters across governance, personnel, information (including ICT) and physical security.	
PSPF Policy 3	B.1		Each entity must have in place a security plan approved by the accountable authority to manage the entity's security risks.	
PSPF Policy 3	B.1		The security plan details the:	a. security goals and strategic objectives of the entity, including how security risk management intersects with and supports broader business objectives and priorities
PSPF Policy 3	B.1			b. threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets
PSPF Policy 3	B.1			c. entity's tolerance to security risks
PSPF Policy 3	B.1			d. maturity of the entity's capability to manage security risks, and
PSPF Policy 3	B.1			e. entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.
PSPF Policy 3		Requirement 2. Critical assets	Entities must identify people, information and assets that are critical to the ongoing operation of	

[1] Note: Accredited entities may consider the guidance advice in section C.9.4 of PSPF Policy 2 for implementation of this requirement

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
			the entity and the national interest and apply appropriate protections to these resources to support their core business.	
PSPF Policy 3		Requirement 3. Risk steward	Entities must identify a risk steward (or manager) who is responsible for each security risk or category of security risk, including for shared risks.	
PSPF Policy 3		Requirement 5. Threat levels	The security plan (and supporting security plans) must include scalable measures to meet variations in threat levels and accommodate changes in the National Terrorism Threat Level.	
PSPF Policy 3		Requirement 6. Alternative mitigations	Where the CSO (or security advisor on behalf of the CSO) implements an alternative mitigation measure or control to a PSPF requirement, they must document the decision and adjust the maturity level for the related PSPF requirement.	
PSPF Policy 4	B.1		Each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan.	
PSPF Policy 4		Requirement 1. Security maturity records	Entities must document and evidence their assessment of the entity's security maturity.	
PSPF Policy 6			Each entity is accountable for the security risks arising from procuring goods and services, and must ensure contracted providers comply with relevant PSPF requirements.	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 6		Requirement 1. Assessing and managing security risks of procurement	When procuring goods or services, entities must put in place proportionate protective security measures by identifying and documenting:	a. specific security risks to its people, information and assets, and
		Requirement 1.		b. mitigations for identified risks.
PSPF Policy 6		Requirement 2. Establishing protective security terms and conditions in contracts	Entities must ensure that contracts for goods and services include relevant security terms and conditions for the provider to:	a. apply appropriate information, physical and personnel security requirements of the PSPF
PSPF Policy 6		Requirement 2.		b. manage identified security risks relevant to the procurement, and
PSPF Policy 6		Requirement 2.		c. implement governance arrangements to manage ongoing protective security requirements, including to notify the entity of any actual or suspected security incidents and follow reasonable direction from the entity arising from incident investigations.
PSPF Policy 6		Requirement 3. Ongoing management of protective security in contracts	When managing contracts, entities must put in place the following measures over the life of a contract:	a. ensure that security controls included in the contract are implemented, operated and maintained by the contracted provider and associated subcontractor, and
PSPF Policy 6		Requirement 3.		b. manage any changes to the provision of goods or services, and reassess security risks.

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 6		Requirement 4. Completion or termination of a contract	Entities must implement appropriate security arrangements at completion or termination of a contract.	
PSPF Policy 8			Each entity must:	a. identify information holdings
PSPF Policy 8				b. assess the sensitivity and security classification of information holdings, and
PSPF Policy 8				c. implement operational controls for these information holdings proportional to their value, importance and sensitivity.
PSPF Policy 8		Requirement 7. Storage	Entities must ensure sensitive and security classified information is stored securely in an appropriate security container for the approved zone in accordance with the minimum protection requirements set out in Annexes A to D.	
PSPF Policy 8		Requirement 8. Transfer	Entities must ensure sensitive and security classified information is transferred and transmitted by means that deter and detect compromise and that meet the minimum protection requirements set out in Annexes A to D.	
PSPF Policy 8		Requirement 9. Disposal	Entities must ensure sensitive and security classified information is disposed of securely in accordance with the minimum protection requirements set out in Annexes A to D. This includes ensuring sensitive and classified	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
			information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.	
PSPF Policy 9	B.1		Each entity must enable appropriate access to official information. This includes:	a. sharing information within the entity, as well as with other relevant stakeholders
PSPF Policy 9	B.1			b. ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information, and
PSPF Policy 9	B.1			c. controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.
PSPF Policy 9		Requirement 5. Managing access to information systems	To manage access to information systems holding sensitive or security classified information, entities must implement unique individual identification, authentication and authorisation practices on each occasion where system access is granted.	
PSPF Policy 11	B.1		Each entity must ensure the secure operation of their ICT systems to safeguard their information and data and the continuous delivery of government business by applying the Information Security Manual's cyber security principles during all stages of the lifecycle of each system.	
PSPF Policy 11		Requirement 1. Authorisation of ICT systems to operate	Entities must only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
			authorised to operate based on the acceptance of the residual security risks associated with its operation.	
PSPF Policy 11		Requirement 1. Authorisation of ICT systems to operate	Entities must only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation. When establishing new ICT systems, or implementing improvements to an existing system, the decision to authorise (or reauthorise) a system to operate must be based on the Information Security Manual's six step risk-based approach for cyber security.	
PSPF Policy 11		Requirement 4. Vulnerability Disclosure Program	Entities must have in place a vulnerability disclosure program.	
PSPF Policy 12	B.1		Each entity must ensure the eligibility and suitability of its personnel who have access to Australian Government resources (people, information and assets).	
PSPF Policy 12		Requirement 1. Pre-employment screening	Entities must undertake pre-employment screening, including:	a. verifying a person's identity using the Document Verification Service
PSPF Policy 12		Requirement 1.		c. obtaining assurance of a person's suitability to access Australian Government resources, including

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
				their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm.
PSPF Policy 13	B.1		Each entity must assess and manage the ongoing suitability of its personnel and share relevant information of security concern, where appropriate.	
PSPF Policy 14	B.1		Each entity must ensure that separating personnel:	a. have their access to Australian Government resources withdrawn, and
PSPF Policy 14	B.1			b. are informed of any ongoing security obligations.
PSPF Policy 14		Requirement 1. Sharing security relevant information, debriefs and continuing obligations	Prior to personnel separation or transfer, entities must:	a. notify the Chief Security Officer, or relevant security advisor, of any proposed cessation of employment resulting from misconduct or other adverse reasons
PSPF Policy 14		Requirement 2. Withdrawal of access	On separation or transfer, entities must remove personnel's access to Australian Government resources, including:	a. physical facilities, and
PSPF Policy 14		Requirement 2.		b. ICT systems.
PSPF Policy 14		Requirement 3. Risk assessment	Where it is not possible to undertake required separation procedures, entities must undertake a risk assessment to identify any security implications.	

PSPF Policy Number	B.1 Core	B.2 Supporting requirement	Requirement	Sub-requirement
PSPF Policy 15			Each entity must implement physical security measures that minimise or remove the risk of:	a. harm to people, and
PSPF Policy 15				b. information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
PSPF Policy 15		Requirement 1. Physical security measures	Entities must put in place appropriate physical security measures to protect entity resources, commensurate with the assessed business impact level of their compromise..	
PSPF Policy 15		Requirement 2. Security containers, cabinets and rooms	Entities must assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.	
PSPF Policy 15		Requirement 3. Disposal	Entities must dispose of physical assets securely.	