EXPLANATORY STATEMENT

Issued by authority of the Minister for Finance

Digital ID Act 2024

Digital ID (Accreditation) Rules 2024

Section 168 of the *Digital ID Act 2024* (the Digital ID Act) provides that the Minister may, by legislative instrument, make rules prescribing matters required or permitted by the Digital ID Act to be prescribed by the rules, or necessary or convenient to be prescribed for carrying out or giving effect to the Digital ID Act.

The *Digital ID (Accreditation) Rules 2024* (the Rules) support the operation of the Digital ID Act which aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses.

Promoting trust in digital ID services (including the function and operation of the Australian Government Digital ID System (AGDIS)), including by ensuring less data is shared and stored, and in a more secure way, will also facilitate economic benefits for, and reduce burdens on, the Australian economy.

The purpose of the Rules is to establish a robust and effective legal framework governing the accreditation scheme, including the obligations of accredited entities approved to operate an accredited digital ID service. In particular, the Rules include details on:

- requirements for applying for accreditation;
- assurance assessments and systems testing, such as security and fraud assessments, penetration testing and useability testing;
- requirements for maintaining accreditation, including protective security, fraud and privacy controls, as well as accessibility and inclusion requirements;
- requirements and controls for each kind of accredited service, including identity service providers (ISP), attribute service providers (ASP) and identity exchanges (IXP);
- requirements for an annual review of an entity's accreditation, including whether the entity continues to comply with the applicable law; and
- other matters relating to accreditation, such as the accreditation conditions on an entity.

Entities have been accredited to provide digital ID services since 2019 under the Australian Government's Trusted Digital Identity Framework (TDIF) arrangements, commonly referred to as the TDIF pilot accreditation program. Over 7 years of consultations on the TDIF, including with entities participating in the TDIF pilot accreditation program, has meant that feedback has been continuously incorporated into the TDIF and more recently, the Rules and Accreditation Data Standards. This has resulted in a robust, best-practice and internationally recognised accreditation framework which sets out requirements to ensure accredited entities

provide secure, convenient, voluntary and inclusive ways for individuals to verify their identity for use in online transactions with government and businesses.

The TDIF pilot accreditation program has been operational for 5 years and entities that participated in the TDIF pilot accreditation program have had the option to transition to the legislated accreditation scheme under the Digital ID Act. The mechanism for this transition is provided by the *Digital ID (Transitional and Consequential Provisions) Act 2024* and supporting rules.

The Digital ID Act allows for the Rules, the *Digital ID (Accreditation) Data Standards 2024* (the Accreditation Data Standards), *Digital ID Rules 2024* (Digital ID Rules) and *Digital ID (AGDIS) Data Standards 2024* (the AGDIS Data Standards) to be made. These instruments are collectively referred to as the rules and standards.

The Digital ID Act includes consultation requirements under section 169 of the Digital ID Act where the Minister proposes to make or amend rules. While the Digital ID Act had not yet commenced at the time of making the Rules the Department of Finance (the Department) nevertheless observed these requirements in undertaking consultation.

An exposure draft of the Rules and accompanying consultation material were released for public consultation from 28 May 2024 to 25 June 2024.

The Department undertook over 30 public consultation sessions in the form of webinars and face-to-face roundtables and bilateral meetings with over 250 parties over the 4-week consultation period. The Department received 42 long form submissions and 27 web-form comments from a range of parties including digital ID service providers, industry associations, consumer groups, privacy and inclusion advocates, government agencies and individuals. These built on previous consultations on the draft Digital ID legislation in late 2023, where 30 long form submissions specifically on the Rules were received.

Before making these Rules, the Minister considered issues raised in consultation responses from stakeholders.

Details of the Rules are set out in **Attachment A**.

The Rules are a legislative instrument for the purposes of the *Legislation Act 2003.*

The Rules rely on section 4 of the *Acts Interpretation Act 1901*, as they are made in contemplation of commencement of section 168 of the Digital ID Act. The Rules commence at the same time as the Digital ID Act.

The Office of Impact Analysis (OIA) has been consulted in relation to the Rules and an Impact Analysis **is not required** as these rules do not create any additional impact other than what has already been assessed in the Impact Analysis for the Digital ID Act. OIA reference number: OBPR23-04323.

A Statement of Compatibility with Human Rights is at **Attachment B**.

The Rules are compatible with human rights, and to the extent that they may limit human rights, those limitations are reasonable, necessary and proportionate.

GLOSSARY

This Explanatory Statement uses the following abbreviations and acronyms.

Abbreviation	***Definition***
Accreditation Data Standards	*Digital ID (Accreditation) Data Standards 2024*
ACSC	Australian Cyber Security Centre
ADA	*Age Discrimination Act 2004*
AGDIS	Australian Government Digital ID System
AL	Authenticator Level
APP	Australian Privacy Principle
ASD	Australian Signals Directorate
ASP	Attribute Service Provider
CoI	Commencement of Identity
Data Standards Chair	Digital ID Data Standards Chair
Digital ID Act	*Digital ID Act 2024*
DVS	Document Verification Service
FCP	Fraud control plan
ICAO	International Civil Aviation Organisation
IP level	Identity Proofing Level
ISM	Information Security Manual
IT system	Information technology system
IXP	Identity Exchange Provider
OAIC	Office of the Australian Information Commissioner
PAD	Presentation Attack Detection
PIA	Privacy Impact Assessment
Privacy Act	*Privacy Act 1988*
Privacy governance code	*Privacy (Australian Government Agencies – Governance) APP Code 2017*
PSPF	Protective Security Policy Framework
the Rules or these Rules	*Digital ID (Accreditation) Rules 2024*
SMS	Short Messaging Service
SSP	System security plan
Transitional Act	*Digital ID (Transitional and Consequential Provisions) Act 2024*
UitC	Use in the Community
Unaccredited ISP	Unaccredited Identity Service Provider

Details of the *Digital ID (Accreditation) Rules 2024*

Chapter 1—Preliminary

Rule 1.1 Name

1.1 This rule provides that the name of these rules is the *Digital ID (Accreditation) Rules 2024* (the Rules).

Rule 1.2 Commencement

1.2 The Rules commence at the same time as the Digital ID Act commences.

Rule 1.3 Authority

1.3 The Rules are made under section 168 of the Digital ID Act for the purposes of the provisions in the Digital ID Act where the term 'Accreditation Rules' occurs.

1.4 Section 168 of the Digital ID Act enables the Minister to make legislative instruments, such as the Rules.

Rule 1.4 Definitions

1.5 This rule sets out the definition of expressions in the Rules.

1.6 Notes 1 and 2 under rule 1.4 relevantly provide that a number of expressions in the Rules are defined in the Digital ID Act or the Accreditation Data Standards, respectively.

1.7 Some expressions are defined within a particular rule itself, where those definitions may be the outcome of several requirements and apply in context of the requirements.

1.8 Certain terms are defined in the Accreditation Data Standards because they are more commonplace in the Accreditation Data Standards.

Discussion of key terms

Material change

1.9 The term 'material change' is defined to include any change that alone or cumulatively with other material changes results in, or is reasonably likely to result in, an impact as described by paragraphs (a) or (b) under that term.

1.10 The terms 'material' and 'adverse' are not defined by the Rules or the Digital ID Act and therefore have their ordinary meaning.

1.11 A material change needs to be one that is real and quantifiable to the degree that it can easily be demonstrated to have, or is likely to have, positively or negatively impacted the entity's accredited services, proposed accredited services or ***DI data environment***; or negatively impacted the entity's compliance with the Digital ID Act, the Rules or the Accreditation Data Standards.

Risk assessment

1.12 These Rules contain rules related to risk assessment and management processes, which are generally the same and replicated throughout the following rules:

- subrule 2.4(5)
- rule 3.18(3)
- subrule 4.7(2)
- subrule 4.25(2)
- subrule 5.23(3)

1.13 The policy intention for each rule is the same. The risk assessment process under these Rules requires that an entity develops and uses a risk matrix based on an established risk management framework or standard. An established risk management framework or standard may include a common framework or standard developed and published by reputable organisations, such as the International Organization for Standardization (ISO) or the United States Department of Commerce's National Institute of Standards and Technology (NIST), and be adapted and appropriate to the kind of industry the entity operates in and the kinds of risks to the entity. Examples of established risk management frameworks or standards include, but are not limited to:

- ISO/IEC 31000 Risk Management
- Commonwealth Risk Management Policy
- COBIT 5 (Control Objectives for Information and Related Technology)
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- NIST Cybersecurity Framework (CSF) 2.0

1.14 The requirements for risk assessments are intentionally broad enough to allow an entity flexibility in implementing an established risk management framework that is relevant for its organisation. The risk management process an entity uses is often an established framework that applies to the organisation as a whole or is adapted from the organisational risk framework for different services the entity may provide (which are not necessarily all accredited services). The risk matrix is a tool that is used in reference to the entity's specific analysis, management and rating of risks as relevant to the entity's organisational risks, DI data environment and accredited services and should include the categorisation of severity of harm and the likelihood of harm occurring. Entities may want to consider this in accordance with rules 4.1 and 4.24 relating to requirements to have and maintain a protective security and fraud capability. One risk matrix can apply to all risks and recommendations in each of the rules where a risk assessment process is required.

1.15 Some of the rules listed above have additional requirements relating to risks and recommendations identified in an assessor's report or other assessment and require an entity to conduct a risk assessment on each risk and recommendation and provide a risk rating and response. This risk rating and response must broadly include details of the action the entity will take to address those risks and recommendations, the

timeframe for implementation of the action and the residual risk rating following completion of the action.

Statement of scope and applicability

1.16 The statement of scope and applicability is a critical document which broadly sets out each requirement in the Rules and the Accreditation Data Standards that apply to an applicant and an accredited entity (referred to collectively below as an entity) and the evidence that demonstrates that the entity will comply, or complies, with those requirements. It is intended to be a living document that changes throughout the lifetime of an entity's accreditation as it is required to be reviewed and updated at each annual review in order to maintain accreditation. How the Rules apply and the evidence that demonstrates that the entity will comply or complies will be dependent on how the entity defines its DI data environment (see rule 2.1) and operational context of its accredited services (as described in the DI data environment). The statement of scope and applicability is required to accompany an application for accreditation and be submitted to the Digital ID Regulator under rule 2.2.

1.17 The statement of scope and applicability will assist the entity and the Digital ID Regulator in understanding, assessing and reviewing an entity's accreditation and the applicability of the Rules and the Accreditation Data Standards in relation to the entity's proposed accredited services or accredited services.

1.18 For example, in relation to Chapter 5 of the Rules, where an entity applies to be accredited as an ISP, its statement of scope and applicability would likely provide that it must comply with Part 5.1, but not Parts 5.2 or 5.3 of the Rules. Similarly, if the scope of that ISP's accreditation enables it to provide reusable digital ID services up to and including IP3, the statement of scope and applicability will need to cover which of the applicable requirements in the Accreditation Data Standards apply to the entity's proposed accredited services. These may include which biometric testing requirements apply (for example source biometric matching testing requirements per section 2.6) and which kinds of authenticators will be used (for example, a multi-factor cryptographic software authenticator at AL2 as per section 3.8).

1.19 An entity is required to review its statement of scope and applicability and ensure it remains updated each year as per rule 4.53. This ensures that an accredited entity maintains its statement of scope and applicability and the Digital ID Regulator remains informed and up-to-date in relation to an entity's scope of accreditation and the evidence that demonstrates how the entity meets and continues to meet its legal obligations.

Rule 1.5 Meaning of *taking reasonable steps*

1.20 This rule prescribes the meaning of the term ***taking reasonable steps*** to ensure an identified outcome.

1.21 Paragraphs 1.5(a) to (e) lists the relevant matters to be taken into account in relation to determining whether steps are, or were at a particular time, reasonably able to be done to ensure the identified outcome. The matters listed are not exhaustive.

1.22 The matters listed in this rule are intended to support accredited entities, any assessor and the Digital ID Regulator to understand what steps should reasonably be taken, or have been taken, to ensure an identified outcome for any requirement that contains the "taking reasonable steps" qualifier. It is important for accredited entities

to be clear as to their obligations in respect of the reasonable steps they must take to meet a requirement. Those steps may change over time, particularly regarding the technology, risks and operational context of the accredited services of the accredited entity.

Rule 1.6 Meaning of *authenticated session*

1.23 This rule prescribes the meaning of ***authenticated session*** for the purposes of subsection 56(3) of the Digital ID Act. While there are no provisions in the Rules that refer to authenticated session, the Accreditation Data Standards and AGDIS Data Standards both contain requirements that refer to the term.

Rule 1.7 Incorporated instruments

1.24 Subrule 1.7(1) generally provides that, unless the contrary intention appears in the provision, a reference to matters contained in an ***incorporated instrument*** is a reference to that instrument as in force or existing from time to time.

1.25 This provision is intended to future-proof incorporated instruments by ensuring that future updates to the instruments are incorporated into the Rules.

1.26 Examples of incorporated instruments in these rules include the PSPF and the ISM, which relate to Australian Government policies on protective and cyber security. Examples also include standards set by internationally recognised organisations such as the ISO's ISO/IEC 29794-5 and the ICAO's ICAO Doc 9303 Standard.

1.27 It is appropriate to incorporate these instruments by reference because they set internationally recognised, up-to-date and consistent benchmarks in the fields of protective security, identity management, biometric technology, accessibility, usability and inclusion for all accredited entities to meet to ensure reliability and quality in their services.

1.28 Subrule 1.7(2) relevantly provides that, unless the contrary intention appears in the Rules, an accredited entity is not required to comply with a change to an incorporated instrument until 12 months after the change has taken effect. The intention of this subrule is to provide an accredited entity with a reasonable period of time to comply with a change to an incorporated instrument, after the change has taken effect. This recognises that an accredited entity may not be able to immediately comply with a change to an incorporated instrument and ensures that entities are provided sufficient time to implement, where required, IT system upgrades or other transitional arrangements to comply with the requirements.

1.29 Subrule 1.7(3) makes clear that the application arrangements enabled by subrule 1.7(2) do not apply if the incorporated instrument is an Act or a legislative instrument. This includes the Accreditation Data Standards, which are not subject to the 12-month period in this rule.

1.30 This rule is authorised by subsection 167(3) of the Digital ID Act.

Table 1: List of incorporated instruments

Rule(s)	Instrument title	Published by	Availability	Where to obtain
5.12(b)	*Certificate revocation list for Australian passports*	Australian Passport Office	Free, online	https://www.passports.gov.au/australian-country-signing-certificate-authority-csca.
3.4	*Essential Eight Assessment Process Guide*	Australian Cyber Security Centre	Free, online	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-assessment-process-guide
3.4	*Essential Eight Maturity Model and ISM Mapping*	Australian Cyber Security Centre	Free, online	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-ism-mapping
5.21	*Guide for Facial Comparison Awareness Training of Assessors*	Facial Identification Scientific Working Group	Free, online	fiswg.org/fiswg_guide_for_facial_comp_awareness_trng_assessors_v1.1_20220617.pdf.
1.4 5.12	*ICAO Doc 9303 Standard*	International Civil Aviation Organisation	Free, online	https://www.icao.int/publications/pages/publication.aspx?docnum=9303
1.4 4.22	*Implementing Certificates, TLS, HTTPS and Opportunistic TLS*	Australian Cyber Security Centre	Free, online	https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/web-hardening/implementing-certificates-tls-https-and-opportunistic-tls
1.4 3.4 4.22	*ISM*	Australian Cyber Security Centre	Free, online	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism
1.4	*ISO/IEC 24745:2022*	International Organization for	Online purchase	https://www.iso.org/standard/75302.html

Rule(s)	Instrument title	Published by	Availability	Where to obtain
4.50(4)		Standardization		
1.4 3.3 4.2 4.4 4.5 4.12	*ISO/IEC 27001:2022*	International Organization for Standardization	Online purchase	https://www.iso.org/standard/27001
1.4 5.17 5.20	*ISO/IEC 29794-5:2010*	International Organization for Standardization	Online purchase	https://www.iso.org/standard/50912.html
1.4 5.17	*ISO/IEC 30107-1:2023*	International Organization for Standardization	Free, online	https://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_IEC_30107-1_2023_ed_2_-_id_83828_Publication_PDF_(en).zip
1.4 4.2 4.3 4.9 4.12 Schedule 5	*PSPF*	Department of Home Affairs	Free, online	https://www.protectivesecurity.gov.au/
4.19	*Strategies to Mitigate Cyber Security Incidents (Essential Eight)*	Australian Cyber Security Centre	Free, online	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents
1.4 3.7 3.15 3.16 4.49	*WCAG 2.1*	World Wide Web Consortium	Free, online	https://www.w3.org/TR/WCAG21/
4.49	*World Wide Web Access: Disability Discrimination Act*	Australian Human Rights Commission	Free, online	https://humanrights.gov.au/our-work/disability-rights/world-wide-web-access-disability-

Rule(s)	Instrument title	Published by	Availability	Where to obtain
	Advisory Notes			discrimination-act-advisory-notes-ver

1.31 The ISO standards referenced are available for purchase through the websites linked in the table above. These standards are not free to access online as they are copyrighted. The Department can facilitate access to view a hard copy of an ISO standard at an office in Australia, by appointment, subject to licensing conditions. If access to the ISO standards is required, please email digitalid@finance.gov.au.

1.32 Although these standards are not free, it is appropriate to incorporate them by reference because they give increased confidence to the Digital ID Regulator and the community that the controls and information presented are suitable and fit for purpose as a minimum baseline for all accredited entities.

1.33 Some free standards contain equivalent controls, however, those standards may not be updated as regularly or robustly as the ISO standards. For instance, biometric technology is a rapidly changing and advancing field. As such, the ISO standards for biometric technology have been updated on a regular 5-year cycle by a panel of independent experts in the fields of biometrics. These standards are also subject to extensive consultation before being published.

1.34 This provides confidence that relevant experts in the field of biometrics have developed and consulted on the standards that are referenced in these Rules. Engaging in a process to develop like-standards would not have been time or cost-effective, and it would create the risk of these standards not being of the same quality as the ISO standards.

Rule 1.8 Application—transitioned accredited entities

1.35 This rule sets out the application of certain provisions for ***transitioned accredited entities***, as defined in rule 1.4. Relevantly, a transitioned accredited entity means an entity taken to be accredited immediately after commencement of the Digital ID Act in accordance with item 2 of Schedule 1 to the Transitional Act.

1.36 The effect of this rule is that the provisions listed in the table of subrule 1.8(1) apply to transitioned accredited entities starting on the day that is 12 months after the day on which these Rules commence. A transitioned accredited entity is still subject to all other rules not specified in subrule 1.8(1).

1.37 The term ‘transitioned accredited entity’ is intended to capture entities who had previously been subject to the TDIF pilot accreditation program and have transitioned to the legislated accreditation scheme. The TDIF pilot accreditation program ran for over 5 years, with accredited entities being subject to the requirements of the TDIF. The Rules are based on the TDIF and while many requirements are similar and have simply been clarified in drafting of the Rules, there are several new or changed requirements, which differ from the TDIF.

1.38 Transitioned accredited entities may need to carry out material changes to their DI data environment and IT systems to be able to comply with these new or changed requirements. For example, an ISP may require time to develop and implement

technical code and useability fixes to its IT system to be able to automatically ensure that individuals under the age of 15 cannot create a digital ID as per rule 5.2 (item 10 in the table in rule 1.8). Additionally, some new or changed rules require accredited entities to have new plans and procedures that require time to develop and implement, such as the new requirement for a logging implementation and monitoring plan as per subrule 4.20(3) and (4) (item 3 in the table in rule 1.8) or for an entity to have a separate privacy management plan for its accredited services as per subrule 4.38(3) (item 5 in the table in rule 1.8). Therefore, it is appropriate to defer the application of these requirements for 12 months to enable transitioned accredited entities sufficient time to upgrade their systems to comply with these requirements.

1.39 Given the rigorous accreditation requirements of the TDIF pilot accreditation program, the risks associated with providing transitioning entities with additional time to comply with these new or changed rules are low.

Rule 1.9 Application—applicants

1.40 This rule relevantly provides for these Rules to apply to an entity that has applied for accreditation under section 14 of the Digital ID Act. It also provides that these Rules apply to that entity at the time the entity applies for accreditation.

1.41 The effect of this rule is to modify the application of certain provisions in these Rules to an applicant for accreditation. Broadly, this rule ensures that certain requirements in Chapters 3, 4 and 5 of the Rules, a provision in the Digital ID Act or the Accreditation Data Standards apply to an applicant for accreditation as if it were an accredited entity. This is to enable the applicant to demonstrate its DI data environment and accredited services have been assessed as compliant with the Digital ID Act and all applicable rules to enable the Digital ID Regulator to be satisfied of certain matters under rule 2.7.

Chapter 2—Applying for accreditation

Rule 2.1 DI data environment

2.1 This rule relevantly provides that, for the purposes of paragraph 15(4)(d) of the Digital ID Act, the Digital ID Regulator must not accredit an applicant unless the Digital ID Regulator is satisfied that the applicant meets the requirements set out in the rule.

2.2 The intention of this rule is to ensure that the Digital ID Regulator, any assessor (see rule 3.2), and the applicant understand exactly where the boundaries of the accredited services lie, and how a particular requirement of the Digital ID Act or the Rules applies to that entity. This is particularly important where an accredited entity uses the same infrastructure, IT systems and/or contractors, in whole or in part, for both accredited services and other aspects of the entity's operations which may include unaccredited services or functions.

2.3 A well-defined DI data environment is critical to:

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

2.4 The Rules aim to be technology agnostic, which means that they recognise that each entity's DI data environment will be different, how the Rules apply to those DI data environments will differ, and that different services will comply in different ways. The accredited entity will determine and provide evidence to the Digital ID Regulator on how its proposed accredited service fulfills and adheres to these Rules, taking into account the entity's defined DI data environment, the nature of the information the entity holds, and the potential risks and threats to such information.

2.5 For example, an ISP generating reuseable digital IDs and using a cloud service provider to store encrypted personal information has different risks compared to an ISP creating one-off digital IDs and holding minimal personal information for up to 30 days for fraud checks before destroying that personal information.

2.6 To demonstrate, in both cases of the example above, the accredited entity must implement and comply with rule 4.19 for the Essential Eight, but how they do so will be dependent on the risks and threats they are required to manage in their IT system, along with how that IT system is defined and configured.

2.7 Similarly, an accredited IXP's operational risks in a digital ID system vary based on the type of information shared, the stakeholders it serves, the digital ID providers involved, and its technical setup for transmitting or facilitating the transmission of data between participants of the digital ID system in which it operates. For example, the application of rule 5.37 will depend on whether the IXP is operating its accredited services on a digital ID system outside of the AGDIS and which includes unaccredited ISPs.

2.8 Determining which rules apply to an entity's accredited services is particularly important in relation to rules around privacy, useability and accessibility contained

in Chapter 4 of the Rules and the relevant provisions of the Digital ID Act. For example, the Digital ID Regulator must be able to understand the boundaries of an accredited entity's DI data environment in relation to the collection, use and disclosure of personal information for public-facing accredited services to assess whether the accredited entity is compliant with the Digital ID Act and Rules in relation to express consent notices.

2.9 Paragraph 2.1(a) requires that the Digital ID Regulator is satisfied that the applicant has correctly identified, defined and documented the boundaries of its DI data environment. This includes the infrastructure owned by, and management provided by, any contractor engaged, or proposed to be engaged, by the applicant to provide an accredited service, or part of an accredited service. Subparagraph 2.1(a)(ii) recognises that an accredited entity is accountable for its supply chain and is ultimately responsible if one of the contracted components of its DI data environment breach the Digital ID Act or the Rules. For instance, if a contractor who manages biometric information collected under the Digital ID Act on behalf of an ISP's accredited service discloses that data to a third party without an individual's consent or the ISP's awareness, then it is intended that the ISP would be in breach of the relevant requirements.

2.10 Additionally, the Rules require an accredited entity to manage risks associated with contracted components of its accredited service, such as requirements for managing cloud service provider tenancy and requirements in relation to biometric information where the biometric matching or PAD technology components may be provided by a third-party contractor.

2.11 Paragraph 2.1(b) requires that the Digital ID Regulator must be satisfied that the entity has limited the boundaries of its DI data environment to the extent practicable, having regard to subparagraphs (i) to (iv). This is particularly important where an entity uses shared infrastructure, has contracted service providers as part of the supply chain for its accredited services, or provides other services that are not accredited services. When the Digital ID Regulator considers whether the entity has practicably limited access to information and segregated its DI data environment from other systems, it may consider, for example:

- an entity's risk management processes and controls related to privacy risks, cyber security risks, and fraud risks;
- in the case of public-facing accredited services, useability and accessibility issues;
- whether the entity has implemented and complies with the rules in respect of that shared infrastructure; and
- whether any contractors or third-parties may provide or access its DI data environment.

2.12 In the case of subparagraph 2.1(b)(i), an accredited entity is not necessarily required to entirely segregate its accredited services or DI data environment from other IT systems or shared infrastructure. However, the Digital ID Regulator will consider how an entity segregates information collected, generated, used, held or disclosed for the purpose of an accredited service and whether the entity can accurately define and categorise that information on shared infrastructure. This is particularly important where the entity may collect, use, hold or disclose personal information

from individuals for the purpose of other services or functions that are not accredited (and in some cases are outside the scope of the accreditation scheme) because that information is not protected by the privacy and consumer protections in the Digital ID Act and the Rules.

2.13 The Rules do not prohibit an entity from providing other digital ID services that are not accredited and do not prohibit an entity from providing other digital ID services (or undertaking other functions) from the same DI data environment that is used to provide the accredited services.

2.14 However, an accredited entity who collects personal information for the purposes of providing accredited services must comply with its obligations under the digital ID legislation. This means that if the accredited entity has generated a digital ID in its DI data environment as part of its accredited services, and then wants to use that digital ID across another digital ID system in which it provides services that are not accredited, the use of that digital ID in the other digital ID system must continue to comply with the requirements under the digital ID legislation, including the Digital ID Act's privacy and other safeguards. This is because the obligations under the digital ID legislation for a digital ID that has been generated by an accredited service apply to an accredited entity, regardless of where the digital ID is being used.

2.15 Put simply, an entity must be able to clearly delineate its accredited services from any other digital ID services, or any other functions or activities of the entity, including when defining the boundaries of its DI data environment from which it provides its accredited services. If it cannot, the Digital ID Regulator may decide that it cannot be satisfied that the entity will be able comply with the Digital ID Act and Accreditation Rules and therefore cannot be accredited.

Rule 2.2 Documents to accompany application

2.16 This rule prescribes the documents that an applicant must provide to the Digital ID Regulator to accompany the entity's application for accreditation. The Digital ID Regulator may require other documents to accompany an application for accreditation as per paragraph 141(1)(c) of the Digital ID Act.

Rule 2.3 Criteria to be met

2.17 This rule sets out the criteria which an applicant for accreditation must meet to become accredited.

2.18 Subrule 2.3(2) requires that, at the time the applicant applies for accreditation, the applicant must have an operational IT system. This means that the applicant must ensure and be able to demonstrate that its IT system is configured to meet all requirements of the Rules. Furthermore, the IT system needs to be configured as if it were servicing live transactions and be in an operational state during assurance assessments, systems testing and other required tests, thereby allowing the Digital ID Regulator to determine if the applicant can adhere to the Digital ID Act and the Rules when active services are delivered in the live environment. To be clear, "operational" in this context is taken to mean a real and demonstrably serviceable and usable IT system that is proposed to provide an applicant's proposed accredited services. The IT system or proposed accredited services cannot be conceptual in nature.

2.19 Subrule 2.3(3) sets out the systems testing, assessments and other kinds of testing that an applicant must have conducted to meet the requirements in this rule.

Rule 2.4 Privacy impact assessment

2.20 This rule prescribes the requirements for a PIA, as required to be conducted by paragraph 2.3(3)(c). The requirements broadly relate to the scope and content of the PIA, the independence and competency requirements of the assessor, and the applicant's response to findings and actions it will take to address risks and recommendations identified in the report.

2.21 Typically conducted before starting a project with high privacy risks, a PIA aims to identify and address privacy risks in projects involving the handling of personal information. A PIA is most effective when conducted before starting a project. However, the PIA required by rule 2.4 also serves as a 'point-in-time' compliance assessment of the applicant's proposed accredited services against the privacy requirements in Chapter 3 of the Digital ID Act and Chapter 4 of the Rules. It also provides relevant analysis of the privacy risks and relevant requirements in Chapter 5 of the Rules for the provision of the applicant's accredited services.

2.22 Subparagraph 2.4(2)(c)(ii) broadly requires an assessment of the applicant's compliance with the privacy requirements in Chapter 3 of the Digital ID Act and Part 4.3 of Chapter 4 of the Rules. This includes the applicant's compliance with the APPs or other applicable privacy obligations as required by sections 35A and 36 of the Digital ID Act and requirements in the privacy governance code which are applicable to accredited entities under rule 4.37.

2.23 A PIA and the applicant's response to the PIA report can assist with identifying any privacy risks that the applicant has not yet mitigated, or recommendations that the applicant has not yet actioned, which may give rise to an unacceptable risk to the privacy of individuals for the purpose of mandatory matters to which the Digital ID Regulator must have regard as specified by paragraph 2.6(1)(c).

2.24 Subrule 2.4(5) prescribes the requirements for the course of action in response to the risks and recommendations identified in the PIA. The intention of this subrule is for the entity to form its own view about the risks and recommendations contained in the PIA and respond with the actions the entity will take to address those risks and recommendations.

2.25 Subrule 2.4(6) broadly prescribes the requirements for the applicant's response to each risk and recommendation. The residual risk rating referred to in subparagraphs 2.4(6)(a)(iii) and 2.4(6)(b)(iii) means the expected risk rating for the relevant risk or recommendation after the applicant has undertaken actions to address that risk or recommendation.

2.26 For an explanation on the risk assessment process and entity response, please see the section under Discussion of Key Terms and in the explanation for rule 3.18, which includes similar requirements to subrules 2.4(5) and (6).

Rule 2.5 Technical testing

2.27 This rule relevantly requires the applicant to have conducted technical testing to verify that the IT system through which it will provide its accredited services includes, and can execute, the necessary functionality to support the operation of its

accredited services and comply with the rules specified in subrule 2.5(2).

2.28 Subrule 2.5(3) relevantly requires the applicant to record appropriate evidence to demonstrate that the requirements prescribed by subrule 2.5(2) have been met. Importantly, this includes that the applicant can map each requirement in subrule 2.5(2) with the tests conducted, and the outcomes of each test. Documentation of evidence must demonstrate that the testing outcomes are robust in terms of criteria, assumptions, limitations and dependencies, methodology, results and how identified failures have been addressed. Applicants should be able to demonstrate that they have strong, integrated methods to remain compliant with IT system related rules throughout ongoing development cycles.

Rule 2.6 Matters to which the Digital ID Regulator must have regard

2.29 This rule prescribes matters for the purposes of paragraph 15(5)(a) of the Digital ID Act, which the Digital ID Regulator must have regard to when deciding whether to accredit an applicant.

2.30 This includes whether the applicant's cyber security and fraud risk tolerance is set at a level that is likely to create unacceptable risks in respect of the proposed accredited services to be provided by the applicant if accredited; and whether the PIA (and the applicant's response) has identified matters that could give rise to an unacceptable risk to the privacy of individuals. An unacceptable risk may be where an assessor, the entity, or the Digital ID Regulator has identified a risk that the applicant has not sufficiently mitigated or for which the timeframe to implement risk treatments may be such that individuals or relying parties may be at significant risk of loss or damages, or in the case of privacy, unacceptable risk to the privacy of an individual, should the risk eventuate in the interim.

Rule 2.7 Matters of which the Digital ID Regulator must be satisfied

2.31 This rule generally provides, for the purposes of paragraph 15(4)(d) of the Digital ID Act, matters of which the Digital ID Regulator must be satisfied before accrediting an entity. The effects of subrule 2.7(1) are that the Digital ID Regulator must be satisfied there is a clear evidential link between the information and documents provided, and the specific requirements of the Digital ID Act, the Rules and any applicable standards of the Accreditation Data Standards. The statement of scope and applicability, which sets out the evidentiary link between the information and documents provided, is intended to assist the Digital ID Regulator in this understanding.

Chapter 3—Assurance assessments and systems testing

3.1 This Chapter sets out the requirements for assurance assessments and systems testing that an entity is required to undertake throughout its accreditation lifecycle, including as an applicant (see rule 2.3), during the annual review process as an accredited entity (see Chapter 6) and when a material change occurs (see rule 6.3).

3.2 Assurance assessments and system testing are intended to assure the Digital ID Regulator that:

- the accredited entity has implemented systems, processes and controls which meet the relevant accreditation requirements; and
- the entity complies with the Digital ID Act and the Rules; and
- any risks and recommendations that the assessor has identified with the entity's DI data environment, IT systems or accredited services have been responded to; and
- where required, the entity has implemented, or will implement, appropriate action to address the identified risks and recommendations.

3.3 The following table broadly outlines each assurance assessment and systems testing requirement in this chapter and broadly describes when an entity is required to undertake the assurance assessment or systems testing and if any additional requirements apply.

Table 2: assurance assessment and system testing requirements

Assurance assessment or systems testing	Additional assessor requirements	Required for applicants (see rule 2.3)	Frequency for accredited entities to review (see chapter 6)	Other considerations
Protective security assessment (rule 3.3)	Yes, see rule 3.3(2) and (3)	Yes	Generally, every 2 years (see rule 6.4(3)) OR As per material change requirements in rule 6.3	
Essential strategies review and report (rule 3.4)	No, see rule 3.4(3)	Yes	Generally, every 2 years as part of the protective security assessment requirements (see paragraph 3.3(1)(c) and subrule 6.4(3)) OR	

Assurance assessment or systems testing	Additional assessor requirements	Required for applicants (see rule 2.3)	Frequency for accredited entities to review (see chapter 6)	Other considerations
			As per material change requirements in rule 6.3	
If a control or strategy is not relevant (rule 3.5)	Yes, see rule 3.3(2) and (3)	Yes, if applicable	Generally, every 2 years as part of the protective security assessment (see paragraph 3.3(1)(c) and subrule 6.4(3)), if applicable	
Fraud assessment (rule 3.6)	Yes, see rule 3.6(2)	Yes	Generally, every 2 years (see rule 6.4(1) and other considerations column) OR As per material change requirements in rule 6.3	Rule 6.4(2) allows an exception to the additional assessor requirements if the entity meets the requirements in that rule.
Accessibility and useability assessment (rule 3.7)	No	Yes	As per material change requirements in rule 6.3	
Penetration testing (rules 3.8, 3.9 and 3.10)	Yes, see rule 3.9	Yes	Generally, every year (see rule 6.5(1))	
Useability testing (rules 3.11, 3.12 and 3.13)	No	Yes, if the applicant has public-facing proposed accredited services (see rule 3.12)	As per material change requirements in rule 6.3	
WCAG testing (rules 3.14, 3.15 and 3.16)	No	Yes, see 3.15(a) and (b)	As per material change requirements in rule 6.3	As per rule 3.15 and 4.49(2) and (3), the WCAG compliance

Assurance assessment or systems testing	Additional assessor requirements	Required for applicants (see rule 2.3)	Frequency for accredited entities to review (see chapter 6)	Other considerations
				requirements apply to public-facing information related to an accredited service and public-facing accredited services and will apply differently to each entity dependent on if it has public-facing accredited services.

Part 3.1—General requirements

Rule 3.1 Entity's obligation

3.4 This rule relevantly requires an accredited entity to ensure that the processes for any assurance assessments or systems testing required by the Rules are compliant with this Chapter, and that the relevant elements of the DI data environment meet the requirements of the Digital ID Act and the Rules relevant to the kind of assurance assessment or systems testing being conducted. Accordingly, relevant requirements within this Chapter are to be read with this rule.

3.5 The purpose of this rule is to confirm the entity's responsibility for ensuring that the relevant assurance assessment and systems testing are appropriately scoped to the entity's DI data environment, relevant rules and requirements in the Digital ID Act.

Rule 3.2 Assessors

3.6 This rule relevantly prescribes the requirements for ***assessors*** undertaking assurance assessments and systems testing, including that the entity provides access to documentation, information, and if required, site or premises relevant to the kind of assurance assessment or systems testing.

3.7 Subrule 3.2(1) relevantly requires that the individual performing the assurance assessments and systems testing (***assessor***) must have the appropriate experience, training and qualifications to conduct that kind of assessment or systems testing. If the rules for a kind of assurance assessment or systems testing prescribe additional requirements relating to the assessor for that kind of assurance assessment or systems testing, then the individual conducting the assurance assessment or systems testing must meet those additional requirements. This is intended to ensure that the assessor's report is complete, accurate and can be trusted and relied upon to present a professional opinion of the entity's compliance with the Rules that each assurance assessment covers and any risks, issues or vulnerabilities in the entity's DI data environment or IT system that the systems testing covers.

3.8 Subrule 3.2(2) relevantly requires that an accredited entity must take reasonable steps to, if requested by the assessor, permit the assessor to have secure online access to documentation and information relevant to the assurance assessment or systems testing, and to undertake a site visit to the location at which the accredited services are or will be provided. The meaning of taking reasonable steps is set out in rule 1.5. This rule enables the assessor to accurately assess the entity's DI data environment and IT systems and other evidence that may be sensitive in nature to ensure that the assessor's report and findings cover all relevant information.

Part 3.2—Assurance assessments

Division 1—Protective security assessment

Rule 3.3 Requirements

3.9 Subrule 3.3(1) sets out the matters that must be reviewed and addressed in a ***protective security assessment*** and associated compliance requirements. Subrules 3.3(2) and (3) set out additional requirements for the assessor and, where applicable for an accredited entity that implements ISO/IEC 27001, requirements in relation to the assessor's accreditation to certify entities against ISO/IEC 27001.

3.10 The purpose of paragraphs 3.3(1)(b), (c) and (d) are to provide independent assurance to the Digital ID Regulator that the findings and results of other protective security related reports support the assessor's overall assessment of the accredited entity's compliance with its chosen protective security framework and the protective security rules in Part 4.1 of Chapter 4. This includes that the results from the penetration testing, essential strategies review and risk-based justification for where a protective security control or strategy is not relevant to an entity (as per rule 3.5) are reviewed and have contributed to an assessor's conclusion that the accredited entity can comply with the protective security rules.

3.11 Subrule 3.3(2) contains additional requirements in relation to the assessor conducting the protective security assessment. These requirements are in addition to the general requirements for the assessor as specified in rule 3.2.

3.12 Paragraphs 3.3(2)(a) and (b) broadly require that the assessor is external to the accredited entity and is independent of the design, implementation, operation or management of the accredited entity's DI data environment or accredited services. Whether an assessor is considered external to the entity or its corporate group will depend on the corporate structure of the entity.

3.13 The intention of this requirement is to ensure an independent and objective assessment of the entity's protective security for its accredited services. One example of an external assessor could be a person who is engaged, on a contract, by the accredited entity to conduct the assessment and who is not an employee of the accredited entity. This is a common practice for accreditation and certification schemes and provides confidence to the Digital ID Regulator that the assessment has not been influenced by individuals who may, for example, seek to benefit from producing a favourable review of the accredited entity's accredited services or who may have existing bias which could influence the final report.

3.14 Subrule 3.3(3) contains additional requirements in relation to the assessor conducting the protective security assessment involving the assessment of the ISO/IEC 27001. This ensures that the assessor has the appropriate skills, training and experience as recognised by Joint Accreditation System of Australia and New Zealand (JASANZ) which is a non-profit accreditation body which accredit the bodies that certify or inspect organisations' management systems, products, services or people. JASANZ operations are overseen by a governing board comprising of 10 members, 6 of whom are appointed by the Australian Government and 3 by the New Zealand Government.

3.15 As with other assurance assessments, the results of the security assessment report must be formally responded to by the accredited entity's accountable executive consistent with rule 3.18.

Rule 3.4 Essential strategies review and report

3.16 This rule prescribes the requirements for an accredited entity to review and report on compliance with the Essential Eight Maturity Model and ISM Mapping document for ISM controls marked maturity level 2 (***essential strategies review and report***).

3.17 The provision of the essential strategies review and report to the assessor for the protective security assessment required by rule 3.3 is important to support the assessor's assessment as to whether the accredited entity complies with rule 4.1 regarding the requirement to have and maintain a protective security capability and rule 4.19 regarding the requirement to implement and comply with specific cyber security risk mitigation strategies

3.18 More specifically, the essential strategies review and report is intended to provide evidence to assist that assessor to determine whether the entity has implemented and complies with the mitigation strategies which have a 'relative security effectiveness rating' marked as 'essential' in the *Strategies to Mitigate Cyber Security Incidents* document published by the ACSC as specified in rule 4.19 (commonly known at the time of publication as the "Essential Eight").

3.19 Each essential strategy is associated with groups of controls and better practices in the ISM that, when implemented together, deliver increased maturity for cyber security risk management in relation to each strategy. There are 3 maturity levels per essential strategy, with each level delivering higher confidence that the strategy achieves its objectives. As per subrule 3.4(1), the Essential Eight Maturity Model and ISM Mapping document lists all the ISM controls that are relevant to maturity level 2.

3.20 The essential strategies review and report can be conducted by a member of the accredited entity's personnel who meets the requirements of subrule 3.4(3). This would, for example, allow an accredited entity's internal audit or cyber security function to perform the assessment if they meet the requirements of that subrule.

3.21 An accredited entity is not necessarily required by this rule or rule 4.19 to implement and comply with all the ISM controls marked maturity level 2. By conducting an assessment against these controls, the entity, the assessor for the protective security assessment and the Digital ID Regulator can understand where security risks or vulnerabilities may lie in the entity's IT system in relation to its implementation of such controls and whether there is sufficient evidence that the entity meets the Essential Eight.

3.22 Subrule 3.4(4) broadly requires that the report must be in the form of the assessment report template located in the ***Essential Eight Assessment Process Guide*****,** which also provides additional guidance on the assessment process itself. This provision broadly requires that the person conducting the review provides their opinion as to whether the accredited entity has implemented and complies with the ISM maturity level 2 controls and that where an alternative control is implemented in accordance with paragraph 3.4(b), the control is described along with its effectiveness at mitigating the relevant cyber security risk that the ISM control would otherwise

mitigate. This evidence is particularly important where the accredited entity may consider that it has implemented and complied with the Essential Eight, but the essential strategies review and report has identified risks in the entity's DI data environment which may lead to or be considered an unacceptable cyber security risk (as per paragraph 2.6(1)(b)). The evidence is also particularly important where a corresponding ISM control may be poorly implemented or is not implemented at all, as this may be considered poor risk management in relation to cyber security risks to an accredited entity's DI data environment.

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

3.23 This rule prescribes the steps that an accredited entity must take if the entity does not consider that a particular control in its chosen protective security framework, or Essential Eight strategy in rule 4.19, is relevant to it and the accredited entity has not, or does not intend to, implement that control or strategy. This rule also works in conjunction with rule 4.6 and is intended to apply to circumstances where a protective security control exists to mitigate a certain risk or threat, and that risk or threat does not apply to an accredited entity. This rule is not intended to allow entities to opt-out of implementing requirements that are merely perceived as difficult to implement.

3.24 Paragraphs 3.5(1)(a) and (b) broadly require an accredited entity to provide a risk-based justification to the assessor to explain why it considers specific controls within their chosen protective security framework, or an Essential Eight strategy in rule 4.19, are not relevant for its DI data environment as well as details of controls or risk strategies that the entity has put in place to manage any residual risk.

3.25 The policy intention of this rule is to recognise that certain requirements may not be appropriate in the context of an accredited entity's DI data environment, and in such circumstances provide entities with the opportunity to provide reasons for not complying with the protective security control or Essential Eight strategy.

3.26 Paragraph 3.5(1)(c) prescribes matters which the accredited entity must ensure the assessor includes in their assessment report. This list of matters is intended to ensure:

- that the assessor has considered all relevant details for why an entity has not implemented a control or strategy; and
- that by not implementing that particular control or strategy, the entity is not exposing its DI data environment, accredited services or individuals to cyber security risks that the implementation of a control or strategy would otherwise mitigate.

3.27 **Scenario example:** In the case of the Essential Eight, a common strategy that all accredited entities may not be required to implement and comply with is the requirement to configure Microsoft Office macro settings. This is because Microsoft Office macro settings may not be included as part of the accredited entity's DI data environment or infrastructure, or the accredited entity may use some other operating system or functions that are not Microsoft products. Where this occurs, an accredited entity is still obligated to undertake a risk assessment and identify the perceived risk that the control would normally mitigate and check whether that risk applies to that accredited entity (as required by paragraph 3.5 (1)(b)). For example, where the

accredited entity uses a Linux operating system instead, the accredited entity would be required to conduct a risk assessment as to whether there are other common risks associated with macros or other similar issues unique to the entity's configuration of that operating system and mitigate those where necessary.

3.28 Subrule 3.5(2) broadly provides that if the assessor does not agree with the accredited entity's decision that the control or strategy is not relevant, the accredited entity must implement the protective security control or Essential Eight strategy.

Division 2—Fraud assessment

Rule 3.6 Requirements

3.29 A fraud assessment is a key mechanism for both the accredited entity and the Digital ID Regulator to gain assurance that the accredited entity has implemented and operates an effective framework of fraud controls for its DI data environment and accredited services that reflect the requirements of the Rules.

3.30 This rule sets out the mandatory reviews and assessments accredited entities must undertake as part of their fraud assessment process, as well as the mandatory requirements of an assessor conducting the assessment. The purpose of subrule 3.6(1) is to provide independent assurance to the Digital ID Regulator that the accredited entity can comply with the fraud control requirements in Part 4.2 of Chapter 4 of these Rules.

3.31 Subrule 3.6(2) contains additional requirements in relation to the assessor conducting the fraud assessment. These requirements are in addition to the general requirements for the assessor as specified in rule 3.2. Paragraphs 3.6(2)(a) and (b) require that the assessor is external to the entity and is independent of the design, implementation, operation or management of the accredited entity's DI data environment or accredited services. Whether an assessor is considered external to the entity or its corporate group will depend on the corporate structure of the entity.

3.32 The intention of this requirement is to ensure an independent and objective assessment of the entity's fraud control processes and capability for its accredited services. An example of an external assessor may be a person who is engaged, on a contract, by the entity to conduct the assessment and is not an employee of the accredited entity. This is a common practice for accreditation and certification schemes and provides confidence to the Digital ID Regulator that the assessment has not been influenced by individuals who may, for example, seek to benefit from producing a favourable review of the entity's accredited services or who may influence the final report.

3.33 If an accredited entity is conducting a fraud assessment as part of its annual review obligations under rule 6.4, subrule 6.4(2) provides an exception to the additional assessor requirements set out in subrule 3.6(2), provided the accredited entity meets the requirements set out in subrule 6.4(2). Applicants should review rule 6.4(2) to consider whether they meet the requirements to have a fraud assessor who is not required to meet the additional requirements in subrule 3.6(2) for its next fraud assessment.

3.34 As with other assurance assessments, the entity's accountable executive must formally respond to the results of the fraud assessment report, consistent with rule 3.18.

Division 3—Accessibility and useability assessment

Rule 3.7 Requirements

3.35 This rule sets out the requirements for an accessibility and useability assessment for the purposes of subsection 30(1) of the Digital ID Act. An accessibility and useability assessment is a critical step that entities must take to ensure that accredited services are accessible for individuals who experience barriers when creating or using a digital ID.

3.36 This rule prescribes the mandatory elements that an accessibility and useability assessment must review and assess. To determine the scope and application of the requirements and other elements (including testing reports) that the accessibility and useability assessment covers, accredited entities will need to refer to their description of their DI data environment, including whether they are providing public-facing accredited services.

3.37 There are no additional requirements for an accessibility and useability assessor to meet, other than those in rule 3.2. This means an accredited entity may use its own personnel to conduct the assessment within its organisation, for example, by using members of a product development or user experience team, provided the requirements of rule 3.2 are met.

3.38 As with other assurance assessments, the results of the accessibility and useability assessment report must be formally responded to by the accredited entity's accountable executive consistent with rule 3.18.

Part 3.3—Systems testing

Division 1—Penetration testing

3.39 Penetration testing is intended to provide a level of confidence to both the accredited entity and the Digital ID Regulator that the accredited entity's IT system does not include security vulnerabilities that could be exploited by adversaries who may seek to compromise the accredited service or personal information collected, used, disclosed or held by the entity as part of its accredited service.

Rule 3.8 Penetration testing requirements

3.40 This rule requires an assessor to conduct penetration testing of the accredited entity's IT system. Penetration testing is a security assessment method used to evaluate the effectiveness of the implementation of security controls to mitigate unauthorised access within an IT system. This is achieved by simulating attacks that an adversary might attempt on an IT system, which helps to identify vulnerabilities that could be exploited. This rule outlines specific requirements for penetration testing that must be followed by accredited entities providing accredited services.

3.41 Subrule 3.8(5) broadly provides that the penetration testing must be undertaken before the protective security assessment as described in rule 3.3. This is to ensure that the assessor for the entity's protective security assessment in rule 3.3 can review the results of the penetration testing to inform the assessor's assessment of the entity's DI data environment and cyber security risks.

3.42 Penetration testing assists accredited entities to meet the security standards set by the Rules, ensuring regulatory compliance, particularly where the results of the penetration testing indicate that the entity's implementation of appropriate protective security controls results in an IT system with few, if any, vulnerabilities and a robust approach to detecting, mitigating and managing cyber security risks. Penetration testing assists in mitigating cyber security risks and provides supporting evidence relating to an entity's management of risks, such as:

- **Unauthorised Access:** Identifying and closing security gaps prevents attackers from gaining unauthorised access.
- **Data Breaches:** Protects sensitive information from being stolen or compromised.
- **Service Disruption:** Ensures continuity of service by mitigating potential disruptions caused by attacks.

3.43 The scope of the penetration testing tools and techniques required to be undertaken by the assessor in subrule 3.8(2) must broadly include the following types of testing:

- **Egress and Ingress Points Testing:** This involves testing all entry and exit points of the IT system. Testers are expected to penetrate the system through any possible entry points (ingress) and attempt to exfiltrate data or disrupt services through exit points (egress).
- **Non-authenticated Penetration (Black Box) Testing:** This type of testing simulates an external attack without any prior knowledge of the system.

Testers are expected to use publicly available information and tools to try to gain unauthorised access without any prior knowledge or access credentials.

- **Authenticated Penetration (White Box) Testing:** This testing is designed to emulate attacker tools and techniques. This means that the testing must mimic the methods used by likely attackers to find and exploit weaknesses in the system by conducting the following types of testing.

3.44 Some entities may host their IT system or a component of that system within its DI data environment on cloud service infrastructure. The effect of subrules 3.8(3) and (4) is that where an accredited entity uses the infrastructure of a cloud service provider within its DI data environment, the accredited entity must conduct penetration testing on that part of the cloud service infrastructure. The DI data environment would include any infrastructure components owned by, and managed by, a contractor engaged, or to be engaged, by the entity to provide an accredited service, or part of an accredited service. However, if the cloud service provider does not allow the accredited entity to conduct penetration testing on that part of the cloud infrastructure, then the accredited entity must ensure that the cloud service provider conducts the penetration testing in accordance with the requirements in subrule 3.8(4).

3.45 By requiring that penetration testing extends to components of an accredited entity's IT system that may be hosted on cloud service infrastructure, this rule assists the Digital ID Regulator to be confident that the accredited entity appropriately identifies and manages security vulnerabilities and cyber security risks within the contracted cloud service provider infrastructure that may be exploited by malicious attackers.

3.46 Some cloud service providers may restrict the kinds of activities or processes that can be conducted on the cloud service provider's infrastructure, including some kinds of penetration testing. Where a cloud service provider's policies restrict penetration testing of the relevant components of the accredited entity's IT system hosted on the cloud service provider's infrastructure, subrule 3.8(4) broadly requires that an accredited entity must ensure that the cloud service provider itself has completed the relevant penetration testing and meets the scope of the kinds of testing required by subrule (2).

3.47 If a cloud service provider has conducted penetration testing under paragraph 3.8(4)(a), the applicant or accredited entity is required under subparagraph 2.2(b)(iii) or paragraph 6.9(d) respectively to attest that it is satisfied that the penetration testing covers the kind of testing in subrule 3.8(2).

3.48 An attestation from the accredited entity is appropriate because the cloud service provider is unlikely to be able to provide the accredited entity with a detailed penetration testing report as it may contain sensitive information, which could create or exploit any identified vulnerabilities in the cloud service provider's IT system.

3.49 Subrule 3.8(4) only applies where a cloud service provider restricts one or more kinds of penetration testing required under subrule 3.8(2) and is not a general exemption for all penetration testing on an accredited entity's IT system as described within the accredited entity's DI data environment.

Rule 3.9 Penetration testing assessor

3.50 This rule prescribes additional requirements for the penetration testing assessor to ensure the integrity of the assessment. These requirements are in addition to the general requirements for the assessor as specified in rule 3.2.

3.51 Paragraphs 3.9(a) and (b) require that the assessor is external to the accredited entity and is independent of the design, implementation, operation or management of the accredited entity's DI data environment or accredited services. Whether an assessor is considered external to the accredited entity or its corporate group will depend on the corporate structure of the entity.

3.52 The intention of this requirement is to ensure an independent and objective assessment of the entity's protective security for its accredited services. An example of an external assessor may be a person who is engaged, on a contract, by the entity to conduct the assessment and is not an employee of the accredited entity. This is a common practice for accreditation and certification schemes and provides confidence to the Digital ID Regulator that the assessment has not been influenced by individuals who may, for example, seek to benefit from producing a favourable review of the accredited entity's accredited services or who may influence the final report.

Rule 3.10 Penetration testing report

3.53 This rule sets out the contents that must be included in the penetration testing report. This report must capture the findings of the penetration testing and is in addition to the requirements of the report required by rule 3.17.

3.54 The content required by rule 3.10 is necessary to include in a penetration testing report to ensure that the accredited entity is provided with sufficient information to mitigate any risks and vulnerabilities in its IT system and to consider recommendations to improve security controls in its IT system. Additionally, these items are required in the penetration testing report to assist the assessor conducting the security assessment under rule 3.3 to review the results and findings of the penetration testing. The information about tools and processes used to conduct the penetration testing as well as the scope of the penetration testing will support the security assessment assessor's understanding and review of the findings.

3.55 This requirement is related to the protective security assessment requirements in rules 3.3 and 3.4. This means that, in practice, the protective security assessment for each reporting period has to assess the penetration testing results, which is done before finalising the protective security assessment.

Division 2—Useability testing

3.56 The process of useability testing involves having individuals test the public-facing functionality of accredited services by having those individuals try to obtain and use the entity's accredited services. This type of testing focuses on identifying issues with the user experience of the accredited entity's services as well as whether, and if so to what degree, those services can be accessed and used by a diverse range of people within the Australian community, and still operate as intended.

3.57 The term ***public-facing accredited services*** is used throughout Divisions 2 and 3 and is defined in rule 1.4.

Rule 3.11 Accessible and inclusive services

3.58 This rule provides that Division 2 applies for the purposes of subsection 30(1) of the Digital ID Act, which provides that the Accreditation Rules must provide for and in relation to requirements relating to the accessibility and useability of the accredited services of accredited entities. Subsection 30(2) of the Digital ID Act provides for certain matters in relation to accessibility and useability which must be set out in these Rules. Rule 3.12 provides for the rules that must be made under these provisions of the Digital ID Act.

Rule 3.12 Useability testing requirements

3.59 This rule sets out the useability testing requirements of an accredited entity's public-facing accredited services and includes the scope and requirements for what the useability testing must cover.

3.60 Subrule 3.12(1) provides that the testing of an accredited entity's public-facing accredited services must meet 2 requirements. First, the useability testing must identify any adverse issues in the design, useability and accessibility of the service. Secondly, where any adverse issues relating to useability and accessibility are identified, recommendations must be made to improve the public-facing accredited services to address those issues.

3.61 Subrule 3.12(2) sets out the mandatory requirements of useability testing. Paragraph 3.12(2)(b) requires accredited entities to conduct useability testing involving a diverse range of individuals, covering diversity in disability, age, gender and ethnicity. Paragraph 3.12(2)(c) specifies requirements for testing relating to access to accredited services across devices or browsers and platforms.

3.62 The intention is that useability testing focuses on the efficacy and ease of user experience of all user-interactive elements of the DI data environment, including privacy notices (such as express consent screens) and static web pages (such as the entity's privacy policy) that may be accessed by individuals who consume the public-facing accredited services. Where an accredited entity provides offline processes in relation to the provision of their accredited services, such as a shopfront interaction, this would be considered a point of access and a step in the user journey for the accredited entity's public-facing accredited services and therefore be included within the scope of the useability testing.

3.63 The value in useability testing is in ensuring that public-facing accredited services are designed and maintained to reflect inclusivity principles, so that the service can

be readily and easily used by a diverse range of people in the Australian community. The useability test report and accredited entity's response to that report, including mitigation measures for useability and accessibility issues that have been identified will contribute to the Digital ID Regulator's assurance that the entity has taken reasonable steps to ensure that its accredited services are accessible for individuals who experience barriers when creating or using a digital ID, consistent with subsection 30(1AA) of the Digital ID Act and Part 4.4 of the Rules.

Rule 3.13 Useability testing report

3.64 This rule sets out the content that must be included in a useability testing report. This report must capture the findings of the useability testing and is in addition to the requirements of the report per rule 3.17.

3.65 This rule relevantly provides that the report must include a description of the tools, processes and scope of the testing and includes the assessor's findings and recommendations to address accessibility and useability issues, if any, involving the entity's public-facing accredited services. The purpose of this provision is to ensure that the useability testing assessor prepares a useability testing report that contains sufficient detail to give the accredited entity and the Digital ID Regulator confidence that the testing that was undertaken was appropriately scoped, an appropriate methodology was followed, and appropriate tools were used.

Division 3—WCAG testing

3.66 The Worldwide Web Consortium's Web Content Accessibility Guidelines (***WCAG***) have been developed in cooperation with individuals and organisations around the world, with the goal of providing a single shared standard for web content accessibility that meets the needs of individuals and governments. They define accessibility standards designed to make online content (including content accessed on mobile devices) more accessible to all individuals, including those who experience barriers to access information they need.

3.67 Accessibility is measured in terms of the content meeting success criteria at levels 'A', 'AA' or 'AAA' (lowest to highest) where higher accessibility levels include all the requirements of the lower levels.

3.68 WCAG is a standard that is updated and continuously improved. Version 2.1 of WCAG is the version required by the Rules, rather than the more recent version 2.2 dated 5 October 2023. This is because version 2.1 of the standard is considered an appropriate minimum threshold for accredited digital ID services to meet, at the A standard, while requiring accredited entities to take reasonable steps to meet the AA standard. The version of WCAG required by the rules may be updated in the future to consider newer published standards.

3.69 Feedback from stakeholders and the pilot accreditation program highlighted that careful analysis is required for each subsequent version of WCAG before determining whether all or some of its requirements should be incorporated into the Rules. This is because the WCAG standard is designed to be of general application to digital services and it therefore may not always be appropriate for specific digital ID applications, meaning that automatic and full adoption of the latest standard may not always be prudent.

Rule 3.14 Accessible and inclusive services

3.70 This rule provides that Division 3 – WCAG testing applies for the purposes of subsection 30(1) of the Digital ID Act.

Rule 3.15 WCAG testing requirements

3.71 This rule imposes 2 WCAG testing requirements on an accredited entity.

3.72 First, subrule 3.15(1) relevantly provides that the WCAG testing must test the extent to which an accredited entity's public-facing information relating to its accredited services on its web pages (within the meaning of that term in the WCAG) satisfies the Level A Success Criteria specified in WCAG version 2.1 in accordance with subrule 4.49(2).

3.73 Secondly, subrule 3.15(2) relevantly provides that the WCAG testing must test the extent to which an accredited entity's public-facing accredited services and public-facing information related to its accredited services satisfy the Level AA Success Criteria specified in the WCAG version 2.1 in accordance with subrule 4.49(3).

Rule 3.16 WCAG testing report

3.74 This rule sets out the content that must be included in the WCAG testing report. This

report must capture the findings for the WCAG testing and is in addition to the requirements of the report per rule 3.17.

3.75 The intention of this rule is to ensure that the report includes sufficient detail to give confidence in the testing results. Broadly, the report must include a description of the entity's public-facing accredited services and public-facing information related to its accredited services (as described per rule 2.1) that were tested, and the tools and processes used to test WCAG version 2.1 compliance.

3.76 In addition, the report must include the results, which would include any findings and recommendations and identification of any risks to accessibility by individuals when the entity's IT system is in operation. Where an entity is required to take reasonable steps to meet WCAG version 2.1 to the AA standard and fails to meet a control, it may be required to justify why it has not met that control under rule 1.5, which describes what taking reasonable steps involves.

Part 3.4—Reports for assurance assessments and systems testing

Rule 3.17 Assessor's report

3.77 This rule prescribes the content requirements for the assessors' reports for each kind of assurance assessment and systems testing required by Chapter 3.

3.78 The assessor's report is required by rule 6.9 to be submitted to the Digital ID Regulator as part of an accredited entity's annual review if the entity has conducted an assurance assessment or systems testing.

3.79 The intention of this rule is to ensure that assurance assessment and systems testing reports include sufficient detail to give the Digital ID Regulator confidence in the identification of non-compliance findings, risks, and recommendations. This will aid the Digital ID Regulator's assessment of whether the entity can comply with the Rules. This includes demonstrating that the assessor is appropriately qualified and experienced, that reasonable effort was expended in the assessment or systems testing such that the assessor has applied a robust methodology and/or approach, and that the assessor considered sufficient and appropriate evidence in reaching conclusions (such as confirming which elements of the DI data environment were in scope, what documentation was reviewed, which people were interviewed and so on).

Rule 3.18 Entity's response to an assessor's report

3.80 This rule sets out the requirements for an entity's response to an assessor's report.

3.81 Subrule 3.18(1) relevantly provides that an entity must respond in writing to the findings of each report made by an assessor in the various assurance assessment and system testing reports. Subrule 3.18(2) provides that an accredited entity's written response must be signed by its accountable executive.

3.82 Subrules 3.18(3) and (4) set out the actions that an accredited entity must take for each risk and recommendation in the assessor's report, and the matters that must be included in the accredited entity's response to each risk needing to be assessed and each recommendation, respectively. Further information on the risk assessment process is provided under the Risk Assessment definition discussion in the Discussion of Key Terms section under Rule 1.4 above.

3.83 The accredited entity does not necessarily need to take action to address every risk and recommendation raised by the assessors in their reports. However, the accredited entity must provide a written response about risks and recommendations that the entity will not address detailing:

- the reasons for the entity's decision not to address the risk;
- any alternative actions to be taken by the accredited entity and the timeframes to do so; and
- the residual risk rating expected to follow implementation of any alternative action.

3.84 The assessor's report can inform the Digital ID Regulator in its consideration of the matters set out in rule 2.6. In particular, the accredited entity's response to an assessor's report will inform the Digital ID Regulator about the entity's tolerance for

risks and whether the level is likely to create an unacceptable risk for its accredited services.

3.85 The details of actions and the timeframes for implementation those actions will be monitored by the Digital ID Regulator as part of annual reviews under rule 6.7.

Chapter 4—Requirements for maintaining accreditation

Part 4.1—Protective security controls

Division 1—Capability

Rule 4.1 Protective security capability

4.1 This rule defines the term ***Protective security capability*** and sets out the requirements for that capability.

4.2 The intention of this rule is to ensure that accredited entities:

- have a foundational understanding of current and emerging cyber security risks related to personnel, processes, IT systems, infrastructure and information assets, including the personal information that the accredited entity collects, uses, generates, holds and destroys within its DI data environment; and
- can manage, improve, adapt and respond to those risks by implementing appropriate controls.

4.3 An accredited entity's protective security capability is specific to the configuration and settings of its accredited services, their DI data environment and the information the accredited entity manages. This means that the cyber security risks to the entity's DI data environment will also be unique to that accredited entity.

4.4 Subrule 4.1(1) defines the protective security capability of an accredited entity. An entity's protective security capability is relevantly defined as its ability to manage the protective security of its DI data environment through its implementation and operation of processes and controls. The entity's ability to manage the protective security of its DI data environment would include allocating adequate budget and resources and providing for management oversight.

4.5 This means that all the controls in the Rules, protective security frameworks, or other bespoke controls the accredited entity implements to manage the protective security of its DI data environment contribute to meeting the core requirement to have and maintain a protective security capability.

4.6 The purpose of allocating adequate budget and resources and providing for management oversight is to ensure the continuous operation of those controls to manage cyber security risks as technology, digital ID services and the risk landscape change over time.

4.7 Subrule 4.1(3) broadly requires entities to take reasonable steps (as defined at rule 1.5) to prevent, detect and deal with cyber security incidents. This subrule works in conjunction with rule 4.15 which requires an accredited entity to implement and maintain appropriate incident monitoring and detection mechanisms related to cyber security incidents. The personnel, physical and information security and risk management requirements prescribed by Part 4.1 of the Rules and protective security frameworks such as ISO/IEC 27001 and PSPF may additionally contribute to prevention, detection and management of cyber security incidents.

Division 2—Protective security frameworks

4.8 This Division prescribes the requirements for accredited entities to implement protective security controls in a manner consistent with certain recognised protective security frameworks.

Rule 4.2 Accredited entities must implement a security framework

4.9 This rule relevantly prescribes that an accredited entity must implement one of the prescribed security frameworks, or an alternative framework, in respect of its accredited services and DI data environment. The intention of this rule is to ensure that an accredited entity complies with a best-practice baseline for protective security which covers governance, risk management, and important technical controls related to security of IT systems.

4.10 Entities are given the option of complying with any one of the security frameworks set out in this rule. Entities can choose to comply with an alternative security framework to the PSPF or the ISO/IEC 27001 in recognition of the fact that there are many security frameworks which contain equivalent requirements that set a similar protective security governance and risk management security baseline to either ISO/IEC 27001 or the PSPF. This will also provide any accredited entity with the flexibility of choosing how it complies with the necessary security requirements, considering the accredited entity's particular circumstances. This rule should be read in conjunction with rule 4.5 which sets out the requirements for an alternative framework.

Rule 4.3 Compliance with the PSPF

4.11 This rule prescribes the controls in the PSPF framework which an accredited entity that implements the PSPF must comply with, subject to rule 4.6.

4.12 For certain terms in the PSPF, this rule has the effect of substituting those terms with terms used within the Rules or Digital ID Act. This is intended to ensure that entities can comply with the relevant PSPF requirements within the context of the Rules and the Digital ID Act. For example, the term "Australian Government resources" in the PSPF, has the same meaning as "DI data environment" in the Rules. This would modify item 52 in Schedule 5 to the Rules to ensure that where an entity has separating personnel (i.e. no longer employed by the entity), those personnel have their access to the entity's DI data environment withdrawn.

4.13 This rule should be read in conjunction with Schedule 5 of the Rules.

Rule 4.4 Compliance with ISO/IEC 27001

4.14 This rule prescribes the requirements that an accredited entity which implements ISO/IEC 27001 must comply with, subject to rule 4.6.

4.15 For certain terms in ISO/IEC 27001, this rule has the effect of substituting those terms with terms used within the Rules or the Digital ID Act. This is intended to ensure that entities can comply with the relevant ISO/IEC 27001 requirements within the context of the Rules and the Digital ID Act.

Rule 4.5 Implementation and compliance with an alternative framework

4.16 This rule prescribes the requirements that an accredited entity must meet to implement an alternative framework, subject to rule 4.6. This includes demonstrating that the alternative framework covers, and requires compliance with, the same kinds of controls that the entity would have to comply with had they implemented the PSPF or the ISO/IEC 27001.

4.17 To demonstrate that the alternative framework is comparable to the PSPF or the ISO/IEC 27001, the accredited entity must map the controls in the alternative framework against the corresponding controls in the PSPF or the ISO/IEC 27001 as required by subrules 4.5(2) and (3), respectively. If the alternative framework does not require compliance with a control or controls in the PSPF or ISO/IEC 27001, this rule requires the accredited entity to specify that control in the PSPF or ISO/IEC 27001.

4.18 Subrules 4.5(4) and (5) relevantly provide that if an accredited entity implements an alternative framework, the entity must comply with, and manage and monitor, all the controls specified in that framework and any specific controls in the PSPF or ISO/IEC 27001 that were not able to be mapped to the alternative framework. In addition, where there are new versions of the alternative framework, the accredited entity must also comply with the new version within the timeframe specified for that version or where a timeframe is not specified, 12 months.

4.19 There are many protective security frameworks in operation throughout the world that contain equivalent requirements with ISO/IEC 27001 and the PSPF. The examples given here may not cover all required controls in ISO/IEC 27001 or the PSPF and are provided as an example only:

- The ISM
- The NIST CSF 2.0
- Payment Card Industry Data Security Standard
- MITRE ATT&CK®

Rule 4.6 If a control is not relevant to an entity

4.20 This rule prescribes the circumstances if an accredited entity is not required to comply with a particular control in the framework it implements based on the assessor's opinion set out in the most recent protective security assessment report. This rule operates in conjunction with rule 3.5 to recognise that certain protective security requirements may not be appliable or relevant in the context of the accredited entity's DI data environment, and in such circumstances, it would not be appropriate to require that entity to comply with that particular control.

4.21 This rule only applies to controls in the protective security frameworks. An accredited entity may not apply rule 4.6 to other controls in Part 4.1 of these Rules but should consider the applicability of those controls in the entity's statement of scope and applicability and description of its DI data environment.

Division 3—Additional protective security controls

4.22 This Division prescribes protective security controls in addition to those required by the protective security frameworks described in Division 2. These supplementary controls recognise that additional requirements are needed to address risks specific to the protective security of digital ID services. These requirements are in addition to requirements in the ISO/IEC27001 and PSPF frameworks. Rule 3.3 requires that protective security assessors review and assess an accredited entity's compliance with these additional protective security controls.

Rule 4.7 Cyber security risk assessment

4.23 This rule prescribes that an accredited entity must conduct a ***cyber security risk assessment*** for each reporting period associated with its accredited services and DI data environment. It also prescribes requirements for that risk assessment, including additional requirements if the accredited entity engages with biometric information. This rule recognises that monitoring and responding to a changing cyber security risk profile is fundamental to maintaining a robust security posture. The requirement to conduct a cyber security risk assessment for each reporting period recognises that over time security risks can emerge or change and security control effectiveness can erode.

4.24 For an explanation on the risk assessment process as per subrule 4.7(2), please see the section under Discussion of Key Terms in rule 1.4.

4.25 In practice, a cyber security risk assessment is a systematic evaluation of potential threats and vulnerabilities to an accredited entity's IT systems and DI data environment, aimed at identifying, analysing, and prioritising risks to implement effective security measures and controls to mitigate those risks.

4.26 A cyber security risk assessment process includes the following stages:

- **Risk Evaluation**, the assessment of an entity's cyber security risks according to the entity's risk matrix. The cyber security risks may include common risks but should also include specific risks related to the kinds of services an entity is accredited to provide and risks associated with the configuration of its IT system and supply chain that make up its DI data environment as per rule 2.1.
- **Documentation**, the recording of the results of the risk assessment.
- **Risk Tolerance**, the determination and documentation of an entity's tolerance to cyber security risks. Risk tolerance is generally a level of risk the entity is willing to accept in relation to its risk matrix. Risk tolerance will vary for each entity depending on the services and environment in which it operates. This information may impact the Digital ID Regulator's decision as to whether to accredit an entity as per rule 2.6.
- **Control Measures**, the recording of an entity's controls for mitigating cyber security risks. Many of these control measures may be directly related to requirements and controls an entity implements as part of their compliance with its protective security framework as per rule 4.2. Where risks exist that may not be sufficiently mitigated by existing compliance controls in these

frameworks and the Rules, an accredited entity is expected to address that risk via implementation of other controls.

- **Biometric Information**, if an ISP collects, uses, holds, discloses or destroys biometric information, subrule 4.7(3) broadly requires that the ISP must assess and record in its cyber security risk assessment the associated security risks, mitigation strategies and any other actions the ISP will take to address risks related to biometric information. Biometric information is specifically required to be included as part of the cyber security risk assessment due to its sensitive nature and the associated risks to individuals should biometric information associated with an individual's personal information be compromised. For example, risks associated with reverse engineering biometric matching algorithms if an adversary were to gain access to both the biometric template and a significant volume of raw biometric data.

4.27 Subrule 4.7(4) ensures that if subrule 4.7(1) applies because of rule 2.3, the words 'for each reporting period' in subrule 4.7(1) are ignored for applicants for accreditation. An applicant for accreditation does not have a reporting period, as it only applies to an accredited entity. This purpose of this subrule is to modify subrule 4.7(1) so that it applies to an applicant for accreditation.

Rule 4.8 Sharing information about risks

4.28 This rule relevantly provides for accredited entities to share information about cyber security risks with other participants of the digital ID system(s) in which they operate, as appropriate. How this rule applies to the accredited entity is dependent on its operational environment and the kinds of risks identified. For example, if an ISP provides its accredited services directly to relying parties on a one-to-one contractual basis, and also provides its accredited services in another digital ID system via an IXP, there may be different cyber security risks and circumstances which could be considered appropriate for each kind of operational context.

4.29 The effect of this rule is to broadly require an entity to consider the implications of its decisions relating to cyber security risks and, at its discretion, decide whether sharing information of known cyber security risks or incidents is appropriate.

4.30 Paragraph 4.8(a) relevantly provides for an accredited entity to consider the implications of its decision related to cyber security risk management processes within that digital ID system where those decisions may affect another participant.

4.31 The purpose of paragraph 4.8(b) is to ensure that, as appropriate, and having regard to its considerations under paragraph 4.8(a), the accredited entity shares information on known cyber security risks or cyber security incidents with other participants. This helps ensure all parties involved are informed and can respond to cyber security risks effectively.

4.32 There are different risks and considerations an accredited entity could consider in ensuring compliance with this requirement. For example:

- cyber security risks related to a relying party using the accredited entity's service;

- cyber security risks related to broader vulnerabilities of the risk landscape, including new types of threats or attack vectors which could impact other participants in the Digital ID system in which the entity operates;
- cyber security risks specific to the digital ID system within which the entity is operating and the other participants of that system, for example, risks unique to the types of information that is collected or disclosed in that system; and
- cyber security risks or incidents specific to the accredited entity's provision of accredited services, where the type of information or services may mean there is a heightened risk of attack.

4.33 An accredited entity is only required to share information on known cyber security risks or cyber security incidents with other participants as it is appropriate to do so. The policy intention behind giving an entity the discretion to determine the appropriateness of information sharing is intended to ensure that the accredited entity is not required to share information where it would significantly exacerbate the risk of harm to itself, individuals or to other participants in the digital ID system(s) in which it operates. Where the risk of harm is to the accredited entity itself, it should be balanced against the harm to other participants in the digital ID system in which the entity operates. The appropriate sharing of information could also include considerations of when that information could be appropriately shared, if not immediately.

4.34 For example, when the accredited entity is subject to an active threat, the accredited entity could consider that it is not appropriate to share the information with other participants while the threat is being remediated as doing so could prompt threat actors to exploit the vulnerability. However, after the threat has been remediated, it could be appropriate for the accredited entity to share the information, especially if the threat is a known cyber security risk or incident and could affect the risk profile of other participants. Sharing the information with other participants appropriately in a timely manner would also enable other participants to take necessary steps to deal with those risks.

4.35 The policy intention is that in complying with this rule, entities should act in good faith and share information on known risks as it is appropriate to do so. This policy intention is the same for rule 4.26.

4.36 This rule is intended to foster a collaborative approach to managing cyber security risks and incidents within a digital ID system. By ensuring that information about known risks or incidents is shared with participants, the rule intends to support a well-informed network where every entity and user can take proactive measures to protect itself and the system. Cyber security threats often have a ripple effect; a vulnerability in one part of the system can potentially compromise others. In the context of a digital ID system, an accredited entity is required to evaluate how its cyber security decisions could impact other users within the system. The method for sharing these risks is up to the entity and dependent on the type of risk or incident (for example, the entity may use email, secure messaging or SMS services to inform other participants).

Rule 4.9 Eligibility and suitability of personnel

4.37 This rule prescribes that an accredited entity must take reasonable steps to ensure the ongoing eligibility and suitability of its personnel who interact with the DI data environment. This is to manage the enduring security risk of potential insider threat from employees and contractors.

4.38 An accredited entity is responsible for maintaining the integrity and security of its DI data environment through the regular verification of personnel who manage and interact with the DI data environment. This ensures personnel are only eligible for roles appropriate to their position and supports other protective security controls related to restricting access privileges or administration privileges for vulnerable areas of an entity's IT system.

4.39 Assessing ongoing eligibility and suitability can be achieved through ongoing assessments, in line with the PSPF or the security framework chosen by the entity in accordance with the requirements of the Rules, to ensure staff are up to date with the latest security practices and compliance standards. Additionally, through the ongoing eligibility and suitability checks on personnel, the integrity and security of a DI data environment is maintained. It is critical that entities are aware of changes in their employees' circumstances and workforce behaviours. This awareness is facilitated by effective information sharing and a positive security culture, recognising that security is everyone's responsibility. Effectively assessing and managing ongoing suitability ensures that entities' personnel, including contractors, continue to meet eligibility and suitability requirements established at the point of engagement.

4.40 Ongoing checks may, for example, include requiring personnel to undergo fresh police record checks at set intervals, obtaining periodic declarations from personnel regarding changes of circumstances, annually discussing change of circumstances as part of broader performance discussions with personnel, or other checks appropriate to the accredited entity's industry and business model.

Rule 4.10 Advice to individuals

4.41 This rule requires an ISP to provide advice to individuals who possess a digital ID about how to safeguard their digital ID against cyber security risks and to update that advice as soon as practicable as new risks and threats emerge. This rule and rule 4.29 operate together to ensure an individual is advised regularly on safeguarding their digital ID against cyber security and Digital ID fraud risks.

4.42 This rule only applies to an ISP, as defined in the Digital ID Act. The intention of this rule is to ensure that individuals using a digital ID can be informed by a trusted entity of potential steps to safeguard their digital ID against cyber security risks, including how to mitigate such risks. The types of risks and how an ISP provides such advice will be dependent on the type of digital ID provider the ISP is (i.e. one-off or reusable Digital IDs), the IP levels it provides and how the ISP provides its services (e.g. via a mobile app, webpage or integrated with other services such as in the case of a white-label service). The advice may be provided at the point of digital ID creation, at the point where a digital ID is used to access a relying party service, periodically via trusted channels, or in other ways depending on the configurations of public-facing systems and operational circumstances of the ISP. It must also be provided as soon as practicable as new risks and threats emerge.

4.43 Such advice is important as it assists in protecting individuals from potential harm and fosters trust in digital ID systems by demonstrating responsible and transparent management of cyber security issues. This rule is intended to ensure that individuals have access to ongoing education about emerging threats and best practices in cyber security. By receiving regular updates and advice, individuals can stay informed about the latest risks and how to mitigate them, reducing their vulnerability to cyber-attacks.

Rule 4.11 Support to individuals

4.44 This rule prescribes that accredited entities providing public-facing accredited services must provide support services to individuals who have been adversely affected by a cyber security incident, including, at a minimum, a function that allows individuals to speak with a natural person, and communication channels that include a monitored email, a monitored chat function or a call centre. Additional support services may be provided at the accredited entity's discretion.

4.45 This rule is intended to apply in circumstances where an individual has been adversely affected by a cyber security incident, regardless of the severity of the impact. Support to individuals may include providing guidance to those who have been adversely affected by a cyber security incident and assists in reinforcing the public's trust in digital services.

Subdivision A—System security plan

4.46 This subdivision prescribes the requirements for an entity's system security plan (SSP).

Rule 4.12 Requirements for system security plan

4.47 This rule sets out SSP requirements for all accredited entities, and requirements which only apply to ISPs (subrules 4.12(5) – (8)).

4.48 Subrule 4.12(1) relevantly provides that accredited entities must have, maintain and comply with an SSP that meets the requirements of this Subdivision.

4.49 An SSP is a formal document that outlines an organisation's approach to managing and securing its IT system infrastructure and data. It typically includes detailed information about the security governance, controls, policies, procedures, and guidelines that are implemented to protect the organisation's IT system infrastructure, information assets, such as personal information, and other kinds of information (e.g. event log data) from unauthorised access, use, disclosure, disruption, modification, or destruction. The SSP provides information regarding which security controls the entity requires to mitigate risks and needs to be clear in the linkages between the controls listed in the SSP and the risks identified in entity's cyber security risk assessment described at rule 4.7. The SSP should also document details of the entity's specific implementation of its selected controls, by identifying documents or system configuration items that implement each of the controls listed in the plan (as per requirements in the PSPF or ISO/IEC 27001 frameworks related to SSPs).

4.50 For example, a control which states 'entities must identify a risk steward (or

manager) who is responsible for each security risk or category of security risk, including for shared risks' (as per item 21 of Schedule 5) could be implemented by system governance documentation or position descriptions, and these documents should be referenced against the control in the SSP. Whereas a control which states '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' (as per item 43 of Schedule 5) could be implemented through an access policy or approved procedures for granting, reviewing and removing access, and should have these documents listed against the control in the SSP.

4.51 Subrules 4.12(2) and (3) detail what an SSP must include for an accredited entity that implements either the PSPF Policy 11 (see Schedule 5) or ISO/IEC 27001 respectively. Where the accredited entity chooses an alternative security framework, the accredited entity is required to describe how its system meets all specified requirements in either the PSPF Policy 11 requirement or ISO/IEC 27001 (per rule 4.5).

4.52 The implementation of an SSP ensures the accredited entity adheres to a structured and consistent approach to security governance, controls, policies and procedures. This enables the accredited entity to demonstrate that it has an approach in place to enable adequate protection and risk management against cyber security risks and threats and promotes trust in the entity's security practices.

Goals and strategic objectives

4.53 Subrule 4.12(4)(a) sets out that the SSP must include details of the entity's goals and the strategic objectives to manage and improve its protective security capability. Subrule 4.12(b) requires the entity to set out the activities the entity will undertake to continuously improve that capability.

4.54 Citing the goals and strategic objectives in the SSP provides clear direction and ensures alignment with broader business objectives, making sure that security measures bolster overall operational success. This rule acknowledges that protective security is not a static concept and will always need to adapt to changes and seek to keep ahead of emerging risks and threats. Clearly defined goals help in efficiently allocating resources, focusing efforts on areas with the most impact, and enable accurate performance measurement. This also ensures compliance with regulatory standards and boosts organisational accountability. Additionally, establishing strategic objectives that prioritise adaptability enables the entity to proactively respond to evolving threats, maintaining a strong security posture in a dynamic environment. This rule should be considered in conjunction with the accredited entity's obligations to take reasonable steps to prevent, detect and deal with cyber security incidents by continuously improving its protective security capability under rule 4.1(3)(b) and may help evidence the accredited entity's compliance with that rule.

Destruction of biometric information

4.55 Subrules 4.12(5) and (6) apply to an ISP only and set out the requirements for destroying biometric information.

4.56 If an ISP collects biometric information, the ISP's SSP must include details of processes, procedures, and timeframes for the destruction of this information. This

rule ensures that biometric information, once no longer needed, is irretrievably destroyed, thereby preventing potential misuse or unauthorised access.

4.57 These same requirements apply where another person collects biometric information from, or on behalf of, an ISP.

4.58 Additional obligations apply to accredited entities regarding the collection, use, disclosure and destruction of biometric information under sections 48 to 51 of the Digital ID Act and entities must ensure that the policies and information in their SSP are compliant with the Digital ID Act.

Assessment of risks related to biometric information

4.59 Subrule 4.12(7) applies to an ISP only and sets out the requirements for assessing risks related to biometric information.

4.60 ISPs collecting, using, holding, disclosing or destroying biometric information are responsible for safeguarding an individual's biometric information. The ISP must detail within its SSP any cyber security risks associated with the way the ISP handles and uses biometric information, including risks and mitigation strategies to address those risks associated with the kinds of biometric technology and processes the ISP implements for its accredited services. By doing so, ISPs can better manage and protect biometric information, by addressing cyber security risks related to the unauthorised access to, or misuse of, biometric information.

Use of out-of-band authenticators via PSTN

4.61 Subrule 4.12(8) applies to an ISP only and sets out the SSP requirements for if an ISP authenticates individuals by using out-of-band authenticators via the public switched telephone network (***PSTN***).

Using an out-of-band authenticator via PSTN (i.e., sent over SMS) involves additional risks due to the inherent nature of PSTN (e.g. device swap, SIM change, number porting, or other abnormal behaviour associated with the PSTN). Therefore, an ISP must detail in their SSP the risks and risk management strategies that the ISP will implement if using an out-of-band authenticators via PSTN in its SSP.

Rule 4.13 Review of the system security plan

4.62 This rule broadly requires that an accredited entity must perform a review of the SSP at least once every reporting period (generally 12 months, see rule 6.2), and as soon as practicable after an event listed in paragraph 4.13(1)(b) occurs. The intention of this rule is to ensure the SSP remains relevant and effective in addressing current and emerging cyber security threats.

4.63 In reviewing an SSP, an accredited entity is generally required to:

- have regard to any significant shifts in the entity's cyber security risk and threat and operating environment,
- assess the appropriateness of existing cyber security control measures and mitigation controls and review, and
- review and update strategic objectives and goals accordingly.

4.64 This purpose of this review is to assist with effective ongoing protective security

management and compliance with the Digital ID Act and the Rules. For example, increasing prevalence of phishing as an attack vector might warrant additional investment in staff awareness training specific to preventing, detecting and responding to such threats.

Subdivision B—Cloud service management

4.65 Cloud-based services, including application software services, are increasingly commonplace in modern interconnected systems. Generally, this Subdivision requires that, where cloud services are part of the entity's DI data environment, the entity must demonstrate its management of risks associated with use of the cloud services and that accredited entities have appropriate assurance regarding the effectiveness of protective security controls in place for their cloud service providers.

Rule 4.14 Selection, use and management of cloud services

4.66 This rule relevantly provides the requirements for an accredited entity that uses cloud services as part of its DI data environment to implement. This broadly includes having and maintaining a cloud services management plan and a register of cloud service providers the entity uses. This helps ensure risk mitigation and effective oversight and compliance with security requirements to protect personal information collected, held, used or disclosed using a cloud service.

4.67 Subrule 4.14(1) relevantly requires that an accredited entity that uses cloud services must have and maintain a cloud services management plan that includes policies and processes addressing certain requirements as described in paragraphs (a) to (h). These include but are not limited to selecting, using and managing cloud services, defining and recording all protective security requirements associated with the entity's use of cloud services, and periodic assurance assessments of relevant protective security requirements associated with the cloud services provider. Examples of controls may include geofencing, data encryption, cyber security incident response procedures, service continuity/recovery mechanisms, logging of important security events such as the destruction of data and restricting privileged access to data. Examples of sources of assurance include implementing contractual terms addressing security requirements, documenting service level agreements with periodic performance reporting, certification to relevant standards or an independent assessment report.

4.68 Cloud services can introduce various cyber security risks, including data breaches, loss of data control, and challenges related to data location and access management. The selection, use, and management of cloud services involves developing and maintaining a comprehensive plan that includes policies and processes for choosing appropriate cloud service providers, defining and enforcing security requirements, conducting regular security assessments, responding to incidents, managing data migration, monitoring ongoing security risks, and ensuring complaint handling and destruction of personal information as needed.

4.69 Many cloud service providers publish details of their security certifications so their customers can gain assurance regarding the provider's security posture. Accredited entities should remain informed of the scope of any such certification. Accredited entities should also ensure that any controls the cloud service provider identifies as

being a customer or joint responsibility are included in the accredited entity's own SSP and security management system, and that these controls are assessed by the accredited entity's security assessor. Accredited entities should remain informed of their obligations regarding the selection, use and management of cloud services that intersect with other rules such as the DI data environment requirement, supply chain risk management requirements present in both ISO/IEC 27001 and PSPF frameworks and penetration testing under Chapter 3.

4.70 Subrule 4.14(2) requires the accredited entity to have and maintain a register of cloud services providers whose services it uses which includes information in this provision. This requirement ensures that an accredited entity maintains robust processes and records for the management of cloud services, including information assets and contact information in case of an emergency (such as a data breach or cyber security incident).

Subdivision C—Incident detection, investigation, response and reporting

4.71 This subdivision contains rules regarding cyber security incident detection, investigation, response and reporting.

Rule 4.15 Incident monitoring and detection

4.72 This rule, together with rule 4.16, requires that accredited entities must maintain the capability to manage cyber security incidents. This rule is focused on incident prevention, detection and reporting mechanisms, while rule 4.16 mandates follow-on activities for investigating, managing and responding to incidents.

4.73 Incident monitoring and detection refers to, for example, actively observing network traffic, system logs, and behavioural patterns to identify potential security breaches or anomalies indicative of unauthorised access or malicious activity. The use of "appropriate mechanisms" in subrule 4.15(1) acknowledges that the mechanisms employed by an entity must be adapted and responsive to the entity's operational context, risks of a cyber security incident, and its DI data environment. Incident monitoring and detection enables timely response and actions to minimise impacts from a cyber security event. The incident monitoring and detection mechanism must include an accessible process for reporting actual or suspected cyber security incidents on a confidential basis. The appropriate accessibility of the mechanism is dependent on the type of accredited services and its configurations; for example, whether it is user-facing, back-end, service type, websites or an application.

Rule 4.16 Incident investigation, management and response

4.74 This rule, together with rule 4.15, requires that accredited entities must maintain a cyber security incident management capability where cyber security incidents occur. This rule is focused on investigating and responding to incidents, while rule 4.15 mandates the precursor activities for incident prevention, detection and reporting mechanisms.

4.75 Subrule 4.16(1) relevantly requires that accredited entities must implement and maintain cyber security incident investigation mechanisms within its DI data environment.

4.76 Subrule 4.16(2) relevantly requires that accredited entities must investigate cyber security incidents or suspected cyber security incidents, unless any of those incidents have been referred to, and have been accepted by, an enforcement body or the ACSC.

4.77 Subrule 4.16(3) relevantly provides that, without limiting the requirements in subrule 4.16(1), the incident response mechanisms referred to in subrule 4.16(1) must include processes and procedures to manage and respond to cyber security incidents and suspected cyber security incidents, and, in general terms, the ability for an ISP or ASP (as relevant) to identify, suspend and prevent use of affected digital IDs and special attributes, respectively.

4.78 Incident investigation, management and response refers to the examination of the nature and scope of a security incident, coordinating actions to contain and mitigate damage, and documenting findings and actions taken to address the incident. This purpose of this rule is for accredited entities to have mechanisms and processes in place to support a swift response to cyber security incidents to ensure effective resolution and assist in prevention such events from occurring in the future. Accredited entities should consider this rule in conjunction with record keeping obligations for cyber security incidents in rule 4.18.

Rule 4.17 Disaster recovery and business continuity management

4.79 This rule requires that an accredited entity must have, maintain, and comply with a disaster recovery and business continuity plan for its DI data environment that covers a range of matters as described in paragraphs 4.17(1)(a) to (g). Broadly, the entity must maintain plans for ensuring the continuity of its accredited services, including the recovery of the accredited services from unplanned outages. Disaster recovery and business continuity management refers to the processes and plans an accredited entity has in place to ensure it can recover its DI data environment and minimise impacts on operations in the event of a disruptive incident or disaster, such as a cyberattack, natural disaster, or human error.

4.80 Subrule 4.17(1) prescribes topic areas that must be included in the disaster recovery and business continuity plan.

4.81 Subrule 4.17(2) relevantly provides that the disaster recovery and business continuity plan developed under this rule must be separate from an accredited entity's broader business continuity and recovery plans, such that the DI data environment is explicitly addressed.

4.82 Subrule 4.17(3) mandates that an accredited entity must review and test its disaster recovery and business continuity plan at least once in each reporting period (generally 12 months, see rule 6.2). Testing is required to ensure that the entity has demonstrated that the processes in its plan have been implemented and are effective.

Rule 4.18 Record keeping

4.83 This rule sets out an accredited entity's record keeping obligations where a cyber security incident occurs which causes, or is likely to cause, serious harm to one or more individuals. The records must include the entity's decisions to use civil, administrative or disciplinary procedures, or to take no further action, in response to a cyber security incident of the kind covered in this rule. In practice, this could

include records of whether an investigation into the incident resulted in disciplinary action, civil action, criminal action, or no further action.

4.84 Accredited entities are required to report on cyber security incidents each reporting period. In addition, accredited entities must keep records of any investigations and responses to cyber security incidents that cause, or are likely to cause, serious harm to one or more individuals. The term 'serious harm' is intended to establish a threshold so that accredited entities are not required to record all cyber security incidents that may occur to their accredited services. Due to the nature of information held by accredited entities, they may be the target of thousands of individual attacks per day that fall under the definition of a cyber security incident. Many of these incidents are low level attacks and simplistic in nature, where the attack is repelled by an entity's effective implementation of security controls to mitigate such attacks. An attack that may cause or is likely to cause serious harm to one or more individuals may, for example, be a new kind of cyber attack that increases the cyber security risk to an entity's DI data environment, regardless of whether digital IDs are compromised from that attack. This requirement may intersect with an entity's obligations regarding risk management and the mechanisms under which a review and update of its SSP may occur under rule 4.13.

4.85 To complement the record keeping obligation, for each reporting period an accredited entity must also prepare a report detailing the cyber security incidents that occurred during that period in relation to its accredited services in a digital ID system other than the AGDIS. The information required in the report is listed in subrule 4.18(3). Such reports are not required for the AGDIS because accredited entities providing services in the AGDIS are subject to separate reporting requirements in Chapter 4 of the Digital ID Rules.

4.86 Subrule 4.18(4) requires that, subject to rule 7.8, records to be generated by accredited entities pursuant to this rule be retained for a minimum of 3 years from the date the record was generated and must not contain biometric information. These records are required to be retained for this period of time to assist the Digital ID Regulator with any investigations or directions in relation to the accredited entity's compliance with the Rules.

Subdivision D—Information technology system controls

4.87 This Subdivision sets out the requirements for controls in IT systems that support accredited services.

Rule 4.19 Essential Eight

4.88 This rule lists the required 'Essential Eight' cyber security strategies that accredited entities must implement and comply with.

4.89 The Australian Government, through the ASD, maintains guidance regarding cyber security strategies that are considered the exemplar in mitigating targeted cyber-attacks. The ACSC within the ASD consider that a subset of 8 of these strategies are 'essential' for organisations to implement to make it more difficult for adversaries to compromise an entity's internet-connected systems. These strategies address targeted cyber intrusions (i.e. those executed by advanced persistent threats such as foreign intelligence services), ransomware and external adversaries with destructive

intention, malicious insiders, 'business email compromise', and industrial control systems.

4.90 Through mandating compliance with the Essential Eight strategies, the overall security posture of accredited entities is intended to be improved, assisting in protecting sensitive data and reducing the likelihood of successful cyber security incidents. The boundaries of an accredited entity's DI data environment (rule 2.1) and types of risks to that DI data environment that have been identified (rules 4.1 and 4.7) will inform how the Essential Eight requirements are to be implemented and complied with within the entity's DI data environment.

4.91 Subrule 4.19(2) prescribes the circumstances where an accredited entity is not required to comply with an Essential Eight strategy based on the assessor's opinion set out in the most recent protective security assessment report. This rule operates in conjunction with rule 3.5 to recognise that certain protective security requirements may not be relevant in the context of the accredited entity's DI data environment, and in such circumstances, it would not be appropriate for that entity to comply with the particular requirement of the strategy.

4.92 This rule only applies to the Essential Eight strategies described in subrule 4.19(1). An accredited entity may not apply subrule 4.19(2) to other requirements in Part 4.1 of the Rules but should consider the applicability of those controls in the entity's statement of scope and applicability and description of its DI data environment.

4.93 **Example scenario:** A common mitigation strategy that may not be required to be implemented and complied with for all accredited entities is the requirement to configure Microsoft Office macro settings, which is one of the requirements in the strategy. This is because Microsoft Office macro settings may not be included as part of the accredited entity's DI data environment or the accredited entity may use some other operating system which is unrelated to a Microsoft product. Where this occurs, an accredited entity is still obligated to undertake a risk assessment and identify the perceived risk that the control would normally mitigate and check whether that risk applies to that entity (as required by 3.5).

Rule 4.20 Logging requirements

4.94 This rule sets out the logging requirements for an accredited entity in relation to recording activities, exceptions, faults, and events in its DI data environment. Activities, exceptions, faults and events are to be considered in relation to the entity's accredited services and the operational context of its DI data environment, including the information the entity considers relevant to record and monitor to address risks, issues and compliance with the Digital ID Act and the Rules.

4.95 These logs must capture various critical activities as prescribed by subrule 4.20(2), for example, the handling or destruction of personal and biometric information, changes in access privileges, system alerts related to cyber security risks, and unauthorised access attempts.

4.96 The effect of paragraph 4.20(2)(a) is not to require the log to record an individual's attributes themselves (such as the individual's names and date of birth) but the information about events associated with those attributes, including where those attributes are created, updated, used, disclosed or destroyed. The effect of paragraph 4.20(2)(a) is limited to requiring a log to record that such an activity occurred. For

example, where an individual updated their first and last name associated with their digital ID, a log should record that, in relation to that particular digital ID, attributes related to the individual's first and last name had been verified through source verification and updated at a particular date and time (but not recording the actual first or last name).

4.97 Additionally, accredited entities must develop a logging implementation and monitoring plan that outlines how logs are generated, stored, protected, monitored, and analysed for anomalous behaviour. Event logs that record details of a system's day to day operations and transactions in relation to Digital ID services are critical for effective incident detection, investigation and response. Controls that ensure the integrity and availability of event logs are necessary to support these activities, including minimum retention periods for those event logs.

4.98 Subrule 4.20(4) relevantly requires an accredited entity's logging implementation and monitoring plan to be appropriate and adapted to manage cyber security risks faced by the entity's accredited services and DI data environment. This includes ensuring that the plan is appropriate and adapted to changes in the broader cyber security risk landscape which may include a change in the entity's assessed cyber security risks (as per rule 4.7). For example, if security risks that were previously assessed as unlikely become more likely with the passage of time, events associated with those risks would similarly become more important to log and actively review so that anomalous behaviour can be detected. In this way, the logging and implementation and monitoring plan will remain current and relevant to the accredited entity's circumstances.

4.99 Subrule 4.20(5) prescribes the mandatory details to be included for each log generated under this rule. This rule is intended to enhance the security and accountability of accredited entities by ensuring comprehensive logging of all significant activities, exceptions, faults and events within their DI data environment. Detailed logging helps entities monitor and detect security breaches, track the handling of sensitive information, and respond effectively to incidents.

4.100 Subrule 4.20(6) sets out additional events that must be included in logs required by this rule for the different kinds of accredited services, if the feature or function is supported by the DI data environment.

4.101 Subrule 4.20(7) relevantly provides that event logs containing certain information set out in paragraphs 4.20(2)(a) and (b), (5) and (6) must be retained for a minimum of 3 years from the day it was generated; and explicitly prohibits inclusion of biometric information in event logs. This rule is subject to rule 7.8.

4.102 The kinds of logs that are required to be retained under this subrule are those relating to the creation, update, use, disclosure or destruction of personal information that the accredited entity collects, uses, holds, discloses or destroys, including during digital ID system transactions.

4.103 The purpose of this provision is to enable the Digital ID Regulator to have an appropriate mechanism for enforcement of important privacy and security protections in the Digital ID Act and the Rules related to the personal information that the entity collects, uses, holds, discloses or destroys.

4.104 Information set out in paragraphs 4.20(2)(c) to (f) is not required to be retained for the purposes of subrule 4.20(7). This is because this information is cyber security-

related information and entities are already required to have a plan for analysing the logs and reviewing or escalating suspicious activity like system alerts and failures (as per rule 4.20(3)). That kind of information does not specifically relate to an individual's digital ID, and is instead related to IT system risk management processes and cyber security risk mitigation. Once those logs are actioned appropriately, an entity would usually not retain them as a matter of process and common IT system best practice.

Rule 4.21 Cryptography

4.105 This rule broadly requires that all personal information be encrypted with approved cryptography when at rest within the DI data environment, as well as whenever it is in transit.

4.106 'Cryptography' broadly refers to the practice of securing data, using mathematical algorithms to encrypt and decrypt information to ensure confidentiality, integrity, and authentication. Subsequent rules (4.22 and 4.23) support the use of cryptography and elaborate on the security protections required for its use. The use of approved cryptography assists to safeguard personal information from unauthorised access or disclosures because, even if the data is accessed or breached by a malicious actor, the encryption safeguards mean that the malicious actor may not be able to decrypt the data, therefore adding further layers of protection to personal information.

4.107 Encryption is to be implemented in accordance with the approved cryptography requirements stipulated in the definition for ***approved cryptography*** in rule 1.4. The Rules require the use of cryptographic algorithms and protocols in the ISM, which are regularly monitored and updated by ASD to address emerging technology and new threats. This requirement ensures that accredited entities protect the personal information they collect, use, disclose and hold in accordance with the latest version of those standards.

4.108 **Example scenario:** an accredited entity may hold personal information in a database and secure that whole database with approved cryptography at the database level for the personal information at rest. As threats progress, the accredited entity is considering updating their encryption processes to include encryption at the disk and media level to ensure that even if the database was compromised, the malicious attackers would be required to decrypt items individually (a task that could take several hundred years). When that information is disclosed to another entity, whether an individual, relying party or other third party, that information is encrypted in a package, transmitted and then decrypted at the other end via the use of cryptographic keys. Additionally, to support risk and threat management within the accredited entity's own DI data environment the entity encrypts that information when it is used by the accredited entity within their own network infrastructure.

Rule 4.22 Cryptographic standards

4.109 This rule specifies Transport Layer Security (***TLS***) version 1.3 as one of the cryptographic standards to be used by accredited entities to protect and encrypt personal information in transit, reducing the risk of data breaches and ensure personal information is protected.

4.110 Cryptographic standards, such as TLS, define protocols and algorithms for securing

communications by encrypting data transmissions to prevent interception or tampering, ensuring confidentiality and integrity between the accredited entity and individuals.

4.111 Subrule 4.22(2) allows entities to implement TLS version 1.2 or higher if TLS version 1.3 is not supported, but only if the entity takes appropriate risk mitigation steps consistent with the relevant ACSC publication.

4.112 The reason for this is because TLS version 1.3 is not widely supported by all browsers or devices and the use of TLS version 1.3 may seriously hamper useability for some individuals if they are using an older device to access the entity's accredited services. To balance the protection of personal information with useability and accessibility of a digital ID, this rule requires an accredited entity to consider and implement the latest advice and risk mitigation steps published by ACSC to complement any continuing use of TLS version 1.2 to support the protection of individuals who may not be able to obtain the latest devices that support TLS version 1.3.

Rule 4.23 Cryptographic key management processes and procedures

4.113 This rule requires accredited entities to develop, implement and maintain documented, effective and secure processes and procedures for managing cryptographic keys relevant to the entity's IT system.

4.114 Cryptographic key management processes and procedures involve the generation, distribution, storage, use, and replacement of cryptographic keys used in encryption algorithms to ensure secure and effective protection of personal information. This rule aims to ensure that cryptographic keys, which are fundamental to data security, are managed properly throughout their lifecycle, including protecting them from tampering and access. Effective key management prevents vulnerabilities that could be exploited by adversaries, thereby protecting personal information from potential breaches. For example, if an encrypted database of information was breached but because the entity had poor cryptographic key management processes, the cryptographic keys to decrypt that database were also breached, then the encryption of that information would be rendered ineffective.

Part 4.2—Fraud control requirements

Division 1—Capability

Rule 4.24 Fraud management capability

4.115 This rule defines the term ***fraud management capability*** and sets out the requirements related to that capability.

4.116 The intention of this rule is to ensure that accredited entities understand current and emerging fraud risks relevant to digital ID and their DI data environment, with a view to directing focus on more significant fraud risks with greater impact to individuals and relying parties. However, fraud in any form should always be considered material to an entity and directing focus on more significant fraud risks does not infer that less significant fraud risks can be safely ignored. In addition, this rule provides that an accredited entity must take reasonable steps to prevent, detect and address digital ID fraud incidents.

4.117 Subrule 4.24(3) sets out a non-exhaustive list of steps that an accredited entity must take to demonstrate that they meet the requirements of this provision. As part of the accredited entity's fraud assessment as per Division 2 of Chapter 3, an assessor will consider all the matters in this provision and other relevant matters, including the entity's fraud risk assessment as per rule 4.25, in determining whether the accredited entity has taken reasonable steps to prevent, detect and address digital ID fraud incidents. The intention of this rule is to give the Digital ID Regulator confidence that the accredited entity has and maintains a fraud management capability that can adapt and respond to emerging fraud risks that may cause or contribute to a digital ID fraud incident.

Division 2—Fraud controls

4.118 This Division prescribes the requirements for accredited entities to implement fraud controls.

Rule 4.25 Fraud risk assessment

4.119 This rule requires that an accredited entity must conduct a ***fraud risk assessment*** for each reporting period associated with its accredited services and DI data environment, and the requirements for that risk assessment. It also prescribes additional requirements for the fraud risk assessment if the accredited entity collects, uses, holds, discloses or destroys biometric information.

4.120 The requirement for a fraud risk assessment for each reporting period recognises that over time new fraud risks can emerge or change and fraud control effectiveness can erode.

4.121 The Discussion of Key Terms section also sets out an explanation on the risk assessment process relating to subrule 4.25(2).

4.122 A fraud risk assessment is a systematic evaluation of potential threats and vulnerabilities to an accredited entity's IT systems and DI data environment, aimed at identifying, analysing, and prioritising risks to implement effective fraud control measures and controls to mitigate those risks.

4.123 The fraud risk assessment process involves the following stages:

- **Risk Evaluation**, the assessment of an entity's fraud risks according to the risk matrix.
- **Documentation**, the recording of the results of the risk assessment.
- **Risk Tolerance**, the determination and recording of an entity's tolerance to fraud risks.
- **Control Measures**, the recording of an entity's controls for mitigating fraud risks.
- **Biometric Information**, if an ISP collected, uses, holds, discloses or destroys biometric information, the ISP must assess and record the associated fraud risks, along with mitigation strategies and any other actions the ISP will take to address fraud risks related to biometric information.

4.124 Subrule 4.25(3) relates to the fraud risk assessment where an ISP collects, uses, holds, discloses or destroys biometric information. In these situations, the accredited entity must assess the fraud risks specific to the biometric information and develop associated mitigation strategies and any other actions the ISP will take to address risks related to biometric information. For example, risks related to the accredited entity's technical biometric matching process where the risk of incorrectly matching an individual who is attempting to create a fraudulent digital ID using stolen identity information could be mitigated through robust testing of biometric systems.

4.125 Subrule 4.25(4) ensures that if subrule 4.25(1) applies because of rule 2.3, the words "for each reporting period" in that subrule are ignored for applicants for accreditation. An applicant for accreditation does not have a reporting period, as it only applies to an accredited entity. This purpose of this subrule is to modify subrule

4.25(1) so it applies to an applicant for accreditation.

Rule 4.26 Sharing information about risks

4.126 This rule provides for accredited entities to share information about fraud risks with other participants of the digital ID system(s) in which they operate, as appropriate.

4.127 The purpose of this rule is to ensure that, where appropriate, any known fraud risks or incidents are communicated to other participants in the digital ID system so all parties involved are informed and can respond to fraud risks effectively. It also ensures that an accredited entity has the discretion to decide whether it is appropriate to share information on known fraud risks or incidents with another participant. The policy intention around enabling an entity the discretion to determine whether information sharing is appropriate is the same as outlined in rule 4.8.

4.128 There are different risks and considerations an accredited entity could consider in ensuring compliance with this requirement. For example:

- Fraud risks related to a relying party using the accredited entity's service
- Fraud risks related to broader vulnerabilities of the risk landscape, including new types of threats or attack vectors which could impact other participants in the digital ID system in which the entity operates. For example, new types of available technology which might pose fraud threats to presentation attack detection technology used at higher identity proofing levels.
- Fraud specific to the digital ID system the entity is operating within and the other participants of that system, for example, risks unique to the types of information that is collected or disclosed in that system.
- Fraud risks or incidents specific to the accredited entity's provision of accredited services, where the type of information or services may mean there is a heightened risk of fraud.

Rule 4.27 Fraud controller

4.129 This rule prescribes the requirements for an accredited entity to appoint a fraud controller.

4.130 The fraud controller role is important for enabling effective oversight and governance of an accredited entity's fraud management capability. The role must be held by a senior officer of the accredited entity which is a position with the appropriate level of authority and decision-making that enables that person to manage fraud risks and facilitate the entity's compliance with the fraud control requirements in this Part. This may include approval of mitigation strategies, acceptance of residual fraud risks, receiving periodic assurance that the selected risk mitigation strategies are effective, and having the ability to allocate resources if risk mitigation strategies are found to require adjustment or strengthening.

4.131 Subrule 4.27(3) broadly requires that the person holding the fraud controller role must be appropriately qualified and experienced to effectively carry out their duties. The Rules are not prescriptive in relation to any particular qualification or length and nature of experience. However, accredited entities should be able to provide a rationale as to how their fraud controller meets this requirement.

4.132 Subrule 4.27(4) requires the inclusion of the fraud controller's details in the entity's fraud control plan. The policy intention of this provision is for the fraud controller to be contactable and as such, it is intended for the details to be the name and contact details of the fraud controller.

Rule 4.28 Fraud awareness training

4.133 This rule prescribes the training requirements for an accredited entity's personnel, when the training must occur and the frequency of training. Appropriate training would include information sufficient to educate personnel about fraud risks, fraud concepts in general and individual responsibilities in response to the accredited entity's management of Digital ID fraud incidents, as well as supplementary material to raise awareness of fraud risks that are applicable to the entity's accredited services.

Rule 4.29 Advice to individuals

4.134 This rule requires an ISP to provide advice to individuals who possess a digital ID on how to safeguard their digital ID against fraud risks and to update that advice, as soon as practicable, as new risks and threats emerge. This rule and rule 4.10 operate together to ensure an individual is advised regularly on safeguarding their digital ID against fraud risks.

4.135 This rule only applies to an ISP. The intention of this rule is to ensure that individuals using a digital ID are informed of steps to safeguard their digital ID against fraud risks, including how to mitigate such risks, by the ISP as tailored to their accredited service. The advice may be provided at the point of digital ID creation, at the point where a digital ID is used to access a relying party service, periodically via trusted channels, or in other ways depending on the configurations of public-facing accredited services and operational circumstances of the ISP. It must also be provided as soon as practicable as new risks and threats emerge.

4.136 Such advice is important as it assists in protecting individuals from potential harm from digital ID fraud incidents and fosters trust in digital ID systems by demonstrating responsible and transparent management of fraud issues. This rule is intended to ensure that individuals who use an ISP's accredited services are continuously educated about emerging threats and best practices in fraud risk management, such as common scams techniques that may be used to compromise an individual's digital ID. By receiving regular updates and advice, individuals can stay informed about the latest risks and how to mitigate them, reducing their vulnerability to digital ID fraud incidents.

Rule 4.30 Support to individuals

4.137 This rule prescribes that accredited entities providing public-facing accredited services must provide support services to individuals who have been adversely affected by a digital ID fraud incident. This includes, at a minimum, the ability for individuals to speak with a support person, and communication channels of the kind that must include either a monitored email function, a monitored chat function or a call centre. Additional support services may be provided at the accredited entity's discretion.

4.138 The intention of this rule is that an accredited entity must provide support services to an individual who has been negatively affected by digital ID fraud incident, regardless of the severity of this impact. Support to individuals may offer help and guidance to those who have been adversely affected by a digital ID fraud incident and can assist in reinforcing the public's trust in digital services.

Division 3—Fraud control plan

4.139 This Division sets out the requirements for an entity's FCP.

Rule 4.31 Fraud control plan

4.140 Subrule 4.31(1) requires that an accredited entity must have, maintain and comply with an FCP, and sets out the minimum requirements for that plan.

4.141 An FCP is a formal document that outlines an organisation's approach to managing and mitigating fraud risks and Digital ID fraud incidents for its accredited services. It typically includes detailed information about the fraud control governance, controls, policies, procedures, and guidelines that are tailored, implemented and monitored to protect the entity and individuals from Digital ID fraud risks. It provides information regarding which fraud controls the entity requires to address fraud risks and should be clear in the linkages between the controls listed in the FCP (as per item 1(c) in the table at subrule 4.31(2)) and the risks identified in the entity's fraud risk assessment described at rule 4.25. The FCP should also document details of the entity's specific implementation of its selected controls and risk assessment information, by identifying documents, processes or system configuration items that implement each of the controls listed in the plan.

4.142 The implementation of an FCP enables the accredited entity to adhere to a structured and consistent approach to fraud governance, controls, policies and procedures. This enables the entity to demonstrate that it has an approach in place to enable adequate protection and risk management against fraud risks and threats and promotes trust in the entity's fraud management practices.

4.143 The table in subrule 4.31(2) prescribes the minimum content requirements for the FCP, including:

- an assessment of any fraud risks, threats and vulnerabilities, including their significance;
- the entity's level of tolerance of fraud risks;
- details of strategies and controls to implement and maintain a positive fraud risk culture;
- the entity's key positions with responsibility for managing digital ID fraud risks and duties of those positions;
- goals and strategic objectives to manage and improve its fraud management capability;
- personnel and training requirements; and
- digital ID fraud incident management procedures.

Goals and strategic objectives

4.144 Item 2 in the table sets out the requirements for the goals and strategic objectives for an entity's FCP. The FCP must include details of the entity's goals and the strategic objectives to manage and improve its fraud management capability, and the steps that the entity is taking or proposes to take to continuously improve its fraud management capability.

4.145 Citing the goals and strategic objectives in the FCP provides clear direction and helps to ensure alignment with broader business objectives, so that fraud control measures bolster overall operational success. This rule acknowledges that fraud control is not a static concept and will always need to adapt to changes and seek to keep ahead of emerging risks and threats. Clearly defined goals help in efficiently allocating resources, focusing efforts on areas with the most impact, and enabling accurate performance measurement. This helps ensure compliance with regulatory standards and boosts organisational accountability.

4.146 Additionally, establishing strategic objectives that prioritise adaptability enables the entity to proactively respond to evolving threats, maintaining a strong fraud control posture in a dynamic environment. This rule should be considered in conjunction with the entity's obligations to take reasonable steps to prevent, detect and deal with digital ID fraud incidents by continuously improving its fraud management capability as per paragraph 4.24(3)(b) and may help evidence the entity's compliance with that rule.

Biometric binding and in-device biometric capability

4.147 Items 5 to 9 of the table under subrule 4.31(2) apply to an ISP only and sets out the requirements for the FCP in relation to biometric information.

4.148 An entity continues to be subject to obligations regarding the collection, use, disclosure and destruction of biometric information under sections 48 to 51 of the Digital ID Act and the entity is required to ensure that the policies and information in their FCP are compliant with the Act.

Assessment of risks related to biometric information

4.149 Subrule 4.31(3) broadly identifies the specific elements of the entity's biometric capability that must be considered when developing the entity's FCP. These include biometric matching and binding (including local biometric binding if performed), PAD, and management of biometric information (such as acquired images). An entity is required to include in the FCP details of digital ID fraud risks and associated mitigation strategies and any other actions the entity will take to address fraud risks related to biometric information and the entity's biometric capability. For example, digital ID fraud risks, threats and vulnerabilities specific to the entity's PAD technology such as injection attacks, use of AI deepfake filters or 3D printed masks.

Rule 4.32 Review of entity's fraud control plan

4.150 This rule requires that an accredited entity must review its FCP at least once every reporting period (generally 12 months, see rule 6.2). Subparagraph 4.32(1)(b) sets out additional requirements for when an accredited entity must review and update its FCP outside of the entity's reporting period.

4.151 This rule requires that an accredited entity regularly reviews and updates their FCP, so that the plan remains relevant and effective in addressing current and emerging fraud threats. It broadly requires accredited entities to:

- assess shifts in the digital ID fraud risk landscape, including where there are significant shifts in the entity's threat and operating environment;
- evaluate the effectiveness of existing fraud controls; and

- update strategic objectives and goals accordingly to ensure ongoing fraud control measures are appropriate and the entity continues to comply with the rules.

Division 4—Incident detection, investigation, response and reporting

4.152 This Division sets out requirements in relation to incident detection, investigation, response and reporting.

Rule 4.33 Incident monitoring and detection

4.153 This rule, together with rule 4.34, requires that accredited entities must implement and maintain appropriate mechanisms for digital ID fraud incident detection, management and response. This rule is focused on incident prevention, detection, monitoring and reporting mechanisms, while rule 4.34 mandates follow-on activities for investigating, managing and responding to digital ID fraud incidents.

4.154 Incident monitoring and detection broadly refers to actively observing activities occurring in an entity's DI data environment such as anonymous or other reporting, system logs, behavioural patterns of users or personnel and other external factors. The purpose of these activities is to identify potential anomalies indicative of a compromised digital ID or compromised special attributes being used or disclosed within a digital ID system.

4.155 This rule details the requirements for accredited entities to implement and maintain appropriate mechanisms for digital ID fraud incident monitoring and detection. Incident monitoring and detection enables timely response and mitigation to minimise impacts from use of a compromised digital ID, or compromised special attributes, to access relying party services. The incident monitoring and detection mechanism must include an accessible process for personnel, individuals, enforcement bodies and other entities to report actual or suspected digital ID fraud incidents on a confidential basis. The appropriate accessibility of the mechanism is dependent on the type of accredited services an entity provides. For example, an entity with app-based services could provide a reporting mechanism within its app or on a separate website.

Rule 4.34 Incident investigation, management and response

4.156 This rule, together with rule 4.33, broadly provides for accredited entities to investigate, manage and respond to digital ID fraud incidents that have been suspected or detected by the entity's fraud detection mechanisms. This rule is focused on investigating, managing and responding to incidents, while rule 4.33 mandates the precursor activities for implementing mechanisms to prevent, detect and report digital ID fraud incidents.

4.157 Incident investigation, management and response refers to the examination of the nature and scope of a digital ID fraud incident, coordinating actions to contain and mitigate damage, and documenting findings and actions taken to address the incident.

4.158 This rule aims to ensure that accredited entities are constantly vigilant, allowing for early identification and swift response to potential digital ID fraud incidents to

reduce the harm caused by fraud, whether to individuals who have had their digital ID compromised or to relying parties where a compromised digital ID may have been used to access relying party services.

4.159 Subrule 4.34(2) requires the accredited entity to ensure that its personnel whose duties relate to conducting fraud investigations are appropriately qualified and trained to carry out those duties. The rules are not prescriptive in relation to any particular qualification or length and nature of experience. However, accredited entities should be prepared to provide a rationale as to how their fraud investigators and related personnel meet this requirement.

4.160 Subrule 4.34(3) requires that accredited entities implement and maintain mechanisms for responding to digital ID fraud incidents. These must include procedures that document the entity's processes and include appropriate criteria for making timely decisions at each critical stage in response to a digital ID fraud incident. For example, entities could include criteria to define incident classification and severity levels and set incident response and monitoring pathways for each.

4.161 Subrule 4.34(4) recognises that some accredited entities – such as IXPs - may not hold personal information relevant to the digital ID or attributes that are the subject of a fraud incident. This subrule prescribes that in such circumstances, entities must take reasonable steps, as defined in rule 1.5, to assist other entities participating in the same digital ID system to undertake their investigation into a digital ID fraud incident. The digital ID system referenced in this subrule may be the AGDIS, or another digital ID system. In all cases, an accredited entity operating in any digital ID system (including where the entity is directly connected to relying parties) should ensure that disclosure of such information does not contravene other regulatory requirements such as the Privacy Act.

Rule 4.35 Record keeping

4.162 This rule broadly requires accredited entities to keep records of digital ID fraud incidents and the entity's responses to those incidents. The records must include the accredited entity's decisions to use civil, administrative or disciplinary procedures, or to take no further action, in response to a digital ID fraud incident. In practice, this could include records of whether an investigation into the incident resulted in disciplinary action, civil action, criminal action, or no further action.

4.163 Record keeping refers to maintaining detailed and accurate records of relevant activities, events, and actions taken during the handling of civil, administrative, or disciplinary procedures in response to a digital ID fraud incident. This includes keeping records to ensure transparency and accountability in how accredited entities handle such incidents. Records that are kept serve as crucial documentation for analysis, audit trails, and improvement of incident response processes.

4.164 To complement the record keeping requirements, for each reporting period, an accredited entity must also prepare a report detailing the digital ID fraud incidents that occurred during that period in relation to its accredited services in a digital ID system other than the AGDIS. The information required in the report is listed in subrule 4.35(2). Such reports are not required for the AGDIS because accredited entities providing services in the AGDIS are subject to separate reporting requirements in Chapter 4 of the Digital ID Rules

4.165 Subrule 4.35(3) has the effect of requiring for records in this rule, subject to rule 7.8, to be kept for a minimum of 3 years from the date it was generated and must not contain biometric information. These records are required to be retained for this period of time to assist the Digital ID Regulator with any investigations or directions in relation to the accredited entity's compliance with the Rules.

Part 4.3—Privacy

Rule 4.36 Privacy governance code

4.166 This rule defines the meaning of ***privacy governance code*** to be the *Privacy (Australian Government Agencies – Governance) APP Code 2017* and defines ***agency*** to have the same meaning as in the privacy governance code. These terms are used in rule 4.37.

Rule 4.37 Compliance with privacy governance code

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

4.168 This imposes additional obligations on accredited entities to those in the APPs. The obligations imposed by the privacy governance code operate alongside an accredited entity's obligations under the Rules. They cover matters including an accredited entity's obligations to have a privacy management plan, maintain a privacy policy, and when an entity is required to conduct a PIA.

Rule 4.38 Privacy policy

4.169 This rule broadly sets out the requirements for an accredited entity in relation to its privacy policy and privacy management plan for its accredited services and DI data environment. When developing its privacy policy and privacy management plan, the entity should consider all relevant legal obligations, such as those under the APPs (this includes considering additional requirements for the content of privacy policies set out in APP 1, which continue to apply), the privacy governance code, the Digital ID Act, including sections 53 and 54, and the Rules, including paragraph 2.6(1).

Rule 4.39 Review

4.170 This rule requires an accredited entity to review its privacy policy and privacy management plan at least once in every reporting period.

4.171 This requirement is designed to ensure that an accredited entity's privacy policy and privacy management plan continue to be up-to-date and address any new or emerging privacy risks or issues. This includes meeting the APP requirements and accurately communicating the collection, use, retention and disclosure of personal information as it relates to the DI data environment, as well as any additional obligations stipulated under the Rules and the Digital ID Act.

Rule 4.40 Providing information about express consent

4.172 This rule sets out the requirements for an accredited entity that provides public-facing accredited services and is required to obtain the express consent of an individual. The purpose of this rule is to ensure that individuals are informed about the process for providing, withdrawing or varying consent, so that individuals understand to what they are consenting. This supports an accredited entity to meet its obligations in relation to obtaining express consent when required by the Digital ID

Act.

4.173 The description of the consent process must be clear, simple and accessible and the application of those requirements will depend on the context for the kinds of services an accredited entity provides. The ways in which these terms may apply is dependent on how an accredited entity's accredited public-facing services are configured, the kinds of platforms through which those services are offered (e.g. mobile app, website), and the kinds of individuals who may use those services.

Rule 4.41 Duration of express consent

4.174 This rule prescribes the requirements around any express consent given by an individual, including the consent's duration and prohibits an accredited entity from relying on that consent after it has been withdrawn or has expired.

4.175 An accredited entity with public-facing accredited services must have clear and simple processes in place for an individual to vary or withdraw their consent at any time.

4.176 This rule is consistent with the APP Guidelines, published by the OAIC. Relevantly, these guidelines provide for consent given at a particular time in particular circumstances not to be assumed to endure indefinitely. Consistent with that guideline, the Rules provide for express consent to expire within a specified period of time, which could be as specified by the individual but must not be more than 12 months after the consent was initially given.

4.177 This also allows the individual to experience a more seamless user-experience with their digital ID, for example, where an individual is accessing the same service multiple times, and consents for the same attributes to be provided each time.

Rule 4.42 Data minimisation principle

4.178 This rule sets out the data minimisation principle, which aims to minimise the collection and disclosure of personal information from or via an accredited entity's accredited services. This is designed to ensure that accredited entities provide services that reduce the unnecessary disclosure of personal information to relying parties for the purpose of identity verification.

4.179 Subrule 4.42(1) broadly requires accredited entities to collect only the information that is reasonably necessary to provide their accredited services. This rule complements APP3 and is intended to support the Digital ID Regulator in its assessment of whether an accredited entity's personal information collection may give rise to unacceptable privacy risks for individuals as per rule 2.6(1)(c).

4.180 Subrule 4.42(2) broadly requires accredited entities to support a technical capability to enable relying parties to only select and receive the minimum range of personal information (attributes) that is necessary for the relying party to provide an individual with a service, or access to a service.

4.181 This means that if a relying party only needs an individual's date of birth or age to allow that individual to access the relying party's service, an accredited entity must have the technical capability to be able to only disclose that information, if it is available, and not, for example, any other additional information such as the individual's name or contact details. This does not mean that an accredited entity

cannot offer a bundled attribute option which contains all of those attributes if a relying party requires them; it just means that the accredited entity must also enable relying parties to select and receive a single attribute.

4.182 The operational context of the accredited entity's accredited services and the description of its DI data environment are important to consider in how an accredited entity may meet this rule. For example, if an ISP is operating in a digital ID system where it provides its accredited services via an accredited IXP, the IXP may provide the technical capability on the ISP's behalf. This may mean that the ISP's evidence to meet this requirement is the technical configuration and governance arrangements for the digital ID system in which the ISP operates. To be clear, the obligation to comply with this rule for data minimisation still firmly sits with each accredited entity and as such the obligation to provide evidence for how it maintains data minimisation throughout different operational contexts will need to be met by the accredited entity.

Rule 4.43 Disclosure of personal information for fraud activities

4.183 This rule prescribes the requirement for an accredited entity to notify individuals that their personal information may be used and disclosed to prevent, detect, manage and investigate digital ID fraud incidents. This is intended to promote the transparent operation of accredited services and ensure that an individual is aware and notified of how their information may be used.

4.184 This notification obligation is in addition to other notification obligations that apply under existing privacy regimes.

Rule 4.44 Privacy awareness training

4.185 This rule prescribes the privacy awareness training requirements for an accredited entity's personnel and sets out the requirements for the initial training and the frequency of the training thereafter. This rule is intended to complement the privacy governance code's requirements to provide privacy education and training to personnel by ensuring that, where personnel have specific duties in relation to the accredited entity's accredited services and DI data environment, the privacy training specifically covers relevant information related to those duties as set out in this rule.

Rule 4.45 Data breach response plan

4.186 This rule prescribes the requirement for an entity to have, maintain and comply with a data breach response plan, including the minimum requirements for the plan and requirements to review the plan.

4.187 A data breach response plan is a documented tool and process to help accredited entities prepare for, respond to, contain, assess, notify, review and limit the consequences of a data breach. The plan that is developed and maintained for this rule must include communication and guidance for when notifications will be made within the entity, to individuals affected, and to third parties, including any notifications required by law. This is particularly important for accredited entities to ensure a robust and appropriate response and plan for communication to relevant entities (including individuals) if a data breach occurs in relation to an accredited entity's accredited services.

4.188 Subrule 4.45(3) broadly sets out that an accredited entity's data breach response plan may be an enterprise or organisation level plan, but those plans must comply with this rule, including by requiring the entity to ensure that it covers the matters required for a data breach response plan set out in this rule. This is to ensure that the entity meets, amongst other things, its notification obligations as required by law in its data breach response plan.

4.189 In accordance with subrule 4.45(4) the data breach response plan must be reviewed and, if required, updated at least once in every reporting period.

Rule 4.46 Record keeping

4.190 This rule broadly requires accredited entities to keep records in relation to managing a data breach and the entity's responses to those incidents. The records must include the entity's decisions to use civil, administrative or disciplinary procedures, or to take no further action, in response to a data breach. In practice, this could include records of whether an investigation into the incident resulted in disciplinary action, civil action, criminal action, or no further action.

4.191 Record keeping refers to maintaining detailed and accurate record of relevant activities, events, and actions taken during the handling of civil, administrative, or disciplinary procedures in response to a data breach. This includes keeping records relating to investigation and response, ensuring transparency and accountability in how accredited entities handle such incidents. Records that are kept serve as crucial documentation for analysis, audit trails, and improvement of incident response processes.

4.192 Subrule 4.46(2) has the effect that a record required by this rule must be retained for a minimum of 3 years from the date it was generated and must not contain biometric information, subject to rule 7.8. These records are required to be retained for this period of time to assist the Digital ID Regulator with any investigations or directions in relation to the accredited entity's compliance with the Rules.

Part 4.4—Accredited services must be accessible and inclusive

Rule 4.47 Application

4.193 This rule provides that this Part applies for the purposes of subsection 30(1) of the Digital ID Act.

Rule 4.48 Reporting on accessibility

4.194 This rule prescribes the reporting requirements that an accredited entity must comply with regarding accessibility. This report will assist with demonstrating the entity's compliance with the requirements in subsection 30(1AA) of the Digital ID Act.

4.195 The intention of this rule is to ensure that the Digital ID Regulator is satisfied, as part of the accredited entity's annual review, that an accredited entity continues to take reasonable steps to ensure that its accredited services are accessible for individuals who experience barriers when creating or using a digital ID, in accordance with subsection 30(1AA) of the Digital ID Act.

4.196 This rule acknowledges, similar to the protective security capability and fraud capability rules (see rules 4.1 and 4.25), that reasonable steps for ensuring an accredited service's accessibility may change over time and that accessibility should be considered as requiring continuous improvement and management.

4.197 Paragraph 4.48(b) requires an accredited entity to report on any reasonable steps it proposes to take in the next reporting period to improve the accessibility of its services. To meet this requirement, an entity is expected to consider ways to improve the accessibility of its services and record reasonable steps it proposes to take in the report.

Rule 4.49 Accessibility requirements

4.198 This rule prescribes the accessibility requirements for accredited entities, including in relation to any public-facing information related to accredited services.

4.199 The intention of this rule is to ensure that individuals who may access or use an accredited entity's services have access to clear, simple and easy to understand information about an entity's accredited services and that those accredited services, where public-facing, are accessible to individuals who experience barriers when creating or using a digital ID. It is also intended to ensure that information is accessible and meets specific accessibility standards, as required by section 30 of the Digital ID Act.

4.200 Paragraph 4.49(1)(a) broadly requires an accredited entity to provide individuals with a description of its accredited services and is intended to support transparency for individuals who may access or use an entity's accredited services. This requirement applies to entities whether or not they have a public-facing accredited service; for example, it applies to an IXP. The purpose of this requirement is to ensure that any individual is given information about an accredited entity's accredited services.

4.201 Paragraph 4.49(1)(b) complements paragraph 4.49(1)(a) by ensuring that any public-facing information related to accredited services is presented in a clear and simple

manner, using plain language. The purpose of this rule is to ensure that information provided to individuals is provided in an inclusive manner, by considering its accessibility for a broad range of users who experience different barriers, such as different literacy levels.

4.202 Paragraph 4.49(1)(c) requires an entity to take reasonable steps to ensure that public-facing information in relation to its accredited services is available in multiple accessible formats. The term 'multiple accessible formats' may include, for example, screen-readable web pages, plain English or foreign translations (where, for example, an entity's user base may include a high concentration of members from a culturally and linguistically diverse background).

4.203 Subrule 4.49(2) broadly requires that, for the purposes of paragraph 30(2)(a) of the Digital ID Act, the public-facing information related to an entity's accredited services, which is provided via web pages, must satisfy the Level A Success Criteria specified in WCAG version 2.1. WCAG version 2.1 presents specific success criteria for system accessibility across categories such as 'perceivable', 'operable', 'understandable' and 'robust'.

4.204 Subrule 4.49(3) relevantly provides that an accredited entity with public-facing information related to its accredited services and, should it have them, public-facing accredited services must take reasonable steps to ensure the public-facing information and public-facing accredited services satisfy Level AA Success Criteria as per WCAG version 2.1.

4.205 Subrule 4.49(4) prescribes, for the purposes of paragraph 30(2)(b) of the Digital ID Act, the standards that an accredited entity must have regard to when considering the accessibility of its public-facing accredited services and public-facing information related to accredited services. The intention of this subrule is to ensure an entity considers these standards and has regard to the guidance and information of each standard in relation to the accessibility and continuous improvement of the accessibility of an entity's public-facing accredited services and public-facing information related to accredited services.

4.206 Subrule 4.49(5) relevantly provides that, for the purposes of paragraph 30(2)(e) of the Digital ID Act, an accredited entity providing public-facing accredited services must provide assisted digital support to individuals who may experience barriers when creating or using a digital ID. The entity must also publish details of such support. The intention of this requirement is to ensure that there is support available for individuals when creating or using their digital ID. The appropriate form of assisted digital support will depend on the kinds and configuration of accredited services the entity offers. Publishing the details of the support means that individuals will be able to know it is available and can be accessed if they are having difficulties with accessing or using an entity's public-facing accredited services. Examples of assisted digital support may include, but are not limited to:

- a call centre or telephone support line
- a monitored email address
- a monitored chat function
- a hybrid online and in-person process whereby an individual could attend a shop-front and have a member of the entity's personnel assist.

4.207 Subrule 4.49(6) prescribes the requirements for the written processes and procedures which an entity providing public-facing accredited services must have. These broadly include the requirements that an accredited entity has a process or procedure for individuals to seek assistance and resolve disputes or complaints. Accredited entities are required to obtain and record any feedback from individuals about the usability and accessibility of the entity's public-facing accredited services and, if appropriate, incorporate this feedback into the design of its DI data environment.

4.208 The intention of this requirement is to ensure that entities maintain a continuous improvement cycle and have a way for individuals who may face barriers to accessing an entity's public-facing accredited services to offer suggestions to improve that accessibility.

Part 4.5—Biometric information: testing and fraud activities

Rule 4.50 Requirements if biometric information is used for testing activities

4.209 This rule is made for the purposes of paragraph 49(6)(c) of the Digital ID Act and prescribes the requirements that apply to an accredited entity that uses biometric information for testing purposes.

4.210 Subrule 4.50(2) sets out the purposes for which an entity may conduct testing using biometric information. An entity must not use biometric information for testing purposes beyond those listed in this rule.

4.211 This is intended to limit the uses of biometric information collected and retained to specific purposes that serve to improve an entity's accredited services for the benefit of users. This could include where an entity may use an individual's biometric information to improve false reject rates in biometric matching (i.e. where a legitimate individual has been falsely rejected from an entity's identity proofing or authentication process) or where an entity may use an individual's biometric information to improve the useability of its service. This requirement serves to limit any secondary uses for biometric information collected and retained under the Digital ID Act and enhance privacy protections for an individual's biometric information.

4.212 Subrule 4.50(3) sets out the only circumstances in which such testing may be conducted.

4.213 Paragraph 4.50(3)(a) relevantly provides that entities must not conduct testing using the biometric information of an individual if the entity could instead achieve similar or the same outcomes using relevant and representative synthetic or anonymised biometric data or information. This further limits the circumstances in which it is acceptable for an accredited entity to retain and use biometric information for testing.

4.214 Paragraphs 4.50(3)(b) and (c) also place enhanced protections on using biometric information for testing purposes by, amongst other things, ensuring that accredited entities can carry out the testing in a safe and controlled manner that manages cyber security risks in relation to an individual's biometric information. The purpose of these provisions is to enhance privacy and protective security protections for biometric information.

4.215 Subrule 4.50(4) sets out the information that must be contained in the entity's ***testing plan*** for the biometric information. This covers information relevant for biometric testing such as the methodology for the testing, test frequency and duration, and how the accredited entity will store the biometric information that is held for biometric testing. This is important to ensure that the accredited entity considers its obligations around cyber security risk management and the protection of biometric information used for testing purposes.

4.216 The Note under paragraph 4.50(4)(e) is intended to refer an accredited entity to the option to consider the ISO/IEC 24745 standard for protection of biometric information in relation to the biometric information it holds for testing purposes. To avoid doubt, an accredited entity is not required by this rule to implement this standard.

4.217 Subrule 4.50(5) broadly requires that an accredited entity must conduct any testing using biometric information in accordance with policies covering the ethical use of biometric information, being policies and guidelines that ensure that biometric systems do not selectively disadvantage or discriminate against any group of individuals. The policy intention is to provide entities with the flexibility of developing policies to suit the needs and requirements of their accredited services and the configuration of their biometric technology. However, any policies and guidelines developed by the accredited entity must meet the non-discrimination objective of this subrule, including the collection and retention of an individual's biometric information for testing purposes. The intention of this rule is to ensure that accredited entities consider the circumstances in which an individual's biometric information is collected, retained and used and ensure that the policies and procedures that govern that collection, retention and use do not discriminate against groups of individuals.

4.218 **Example scenario:** An accredited entity wants to collect and retain the biometric information of individuals whom the entity's biometric matching algorithm fails to match. However, this has led to one particular group of individuals of similar demographic backgrounds with the same or similar facial features being flagged as failing the testing algorithm, thereby potentially discriminating against this group of individuals by only using their biometric information to conduct testing to improve the accredited entity's algorithm. While this may be useful to identify in terms of improving the performance of biometric matching for a group of individuals, it may be considered as selectively disadvantaging a particular group because that group's biometric information is disproportionately being flagged for retention and testing. This rule ensures that the accredited entity must consider how all stages of testing using biometric information do not disadvantage particular groups of individuals.

4.219 Subrule 4.50(6) sets out the requirements for reporting the biometric information test results. The purpose of this rule is to ensure oversight and compliance with the requirements in the Rules. Paragraph 4.50(6)(f) generally requires that if an entity is retaining and testing biometric information for the purposes set out in paragraphs 4.50(2)(c), (d) or (f), the entity must report on whether the testing has effectively and ethically detected and corrected bias identified in the biometric technology.

Rule 4.51 Requirements if biometric information is used for fraud activities

4.220 Subsection 49(8) of the Digital ID Act sets out that an accredited entity may retain, use or disclose biometric information of an individual for the purposes of preventing or investigating a digital ID fraud incident. Paragraph 49(8)(c) of the Digital ID Act relevantly provides that such entities must comply with any requirements prescribed by the Accreditation Rules. This rule is made for the purposes of paragraph 49(8)(c) of the Digital ID Act.

4.221 This rule ensures that where an entity uses biometric information for the purposes of preventing or investigating a digital ID fraud incident, it must conduct the digital ID fraud risk management activities in accordance with written ethical principles aimed at avoiding disadvantages to, or discrimination against, individuals. The policy intention is to provide entities with the flexibility of developing principles to suit the needs and requirements of their accredited service and the configuration of their biometric technology. However, any principles developed by the entity must meet the non-discrimination objective of this rule, including the use of an individual's

biometric information for testing purposes. The intention of this rule is to ensure that entities consider the circumstances in which an individual's information is used and ensure that the digital ID fraud risk management activities do not disadvantage or discriminate against individuals.

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

Rule 4.52 DI data environment

4.222 This rule prescribes the requirements for an accredited entity to review and update the documented boundaries of its DI data environment. The purpose of this rule is to ensure that the scope of an entity's DI data environment remains up to date over time, and that this is reflected in the entity's obligations and application of the provisions of the Digital ID Act and Rules. This rule operates in parallel with obligations regarding annual reviews in Chapter 6 of the Rules.

Rule 4.53 Statement of scope and applicability

4.223 This rule prescribes the circumstances and frequency for when an accredited entity must review its statement of scope and applicability. The purpose of this rule is to ensure that the accredited entity can provide the Digital ID Regulator with updated information as part of its annual review and where a material change occurs. This means that the entity's justification and, where applicable, evidence provided to the Digital ID Regulator documenting the entity's compliance with the Rules remains current. This rule operates in parallel with obligations regarding annual reviews in Chapter 6 of the Rules.

Chapter 5—Requirements when providing accredited services

Part 5.1—Accredited identity service providers

5.1 This Part sets out the rules relevant to entities accredited as an ISP.

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

Rule 5.1 General requirements

5.2 This rule prescribes the general requirements that ISPs must meet when generating a digital ID, including requirements set out in this Part and in the Accreditation Data Standards.

5.3 Subrule 5.1(1) sets out the requirements that an ISP must comply with when generating a digital ID. This includes requirements for the identity proofing process relevant to the IP level at which digital ID is being generated.

5.4 Paragraph 5.1(1)(c) relevantly prohibits ISPs from asserting particular IP levels or authentication levels for a digital ID unless the requirements in the ***IP Levels Table*** in rule 5.10 and the ***AL Table*** as defined in the Accreditation Data Standards, have been met.

5.5 Subrule 5.1(2) relevantly prohibits an ISP from asserting that its process for a particular IP level is similar or equivalent to a higher IP level. This means that, for example, an ISP accredited to provide digital IDs up to IP2 cannot claim to offer digital IDs that are equivalent to higher IP levels, even if the proofing processes used in generating those digital IDs meet the requirements in the IP Levels Table. For example, an ISP servicing the financial sector cannot assert that their 'know your customer' (KYC) identity proofing processes are equivalent to (or exceed) IP2 requirements unless the ISP is accredited as an ISP for IP2 (or a higher IP level), and the KYC processes have been accredited as meeting the relevant requirements of the IP Levels Table.

Rule 5.2 Digital IDs and children

5.6 This rule prohibits ISPs from generating a digital ID for individuals under 15 years of age. This minimum age aligns with the OAIC's APP Guidelines made under the Privacy Act, whereby an individual under 15 years of age is presumed to not have capacity to consent. This is important to protect the privacy of children as they may not have the capacity to understand consent and make informed decisions about generating a digital ID. Individuals under 15 years of age can still access government services using alternative ways.

5.7 The ADA prohibits discrimination based on age in accessing government services, unless an exemption applies. The Transitional Act made a consequential amendment to Schedule 2 of the ADA to create an exemption to this prohibition. The effect of this amendment is that anything done by a person in direct compliance with the specified age requirements in the Digital ID Act (including the Rules) is lawful. This means that the minimum age specified in this rule does not contravene the ADA, which is appropriate given the purpose of this rule is to protect the privacy of children.

Rule 5.3 One-off digital IDs

5.8 This rule sets out requirements in relation to ***one-off digital IDs*** (i.e. a 'single use' digital ID that cannot be reused).

5.9 Subrule 5.3(1) relevantly prohibits an ISP accredited to generate a digital ID that is to be used once only from retaining an individual's attributes once it has been disclosed to the relying party.

5.10 The policy intention is for the ISP to delete the attribute as soon as practicable after the transaction has been completed or, if the individual chooses to end the transaction prior to completion, as soon as practicable after the transaction is ended. This rule is intended to enhance privacy protections and protective security risk management for individuals who generate and use a one-off digital ID by limiting data retention periods for these types of digital IDs. This is important for one-off digital IDs as an authenticator is not bound to the digital ID, meaning an individual cannot access or update their attributes or information (as an individual may do as part of reusable digital ID).

5.11 Subrule 5.3(2) provides 2 exceptions to the prohibition in subrule 5.3(1).

5.12 First, an ISP may retain an attribute associated with a one-off digital ID for the purposes of preventing or investigating a digital ID fraud incident for a maximum period of 30 days after the disclosure to the relying party in a transaction. The intention is to balance the privacy of individuals while ensuring that the ISP has sufficient information to conduct fraud investigations, should a digital ID fraud incident be identified or suspected by a relying party or within a Digital ID system.

5.13 Secondly, an ISP must retain the attribute if a law (including the Digital ID Act and the Rules) requires its retention and the attribute is retained in accordance with that law.

Rule 5.4 Use of a reusable digital ID

5.14 Subrule 5.4(1) relevantly prohibits an ISP from allowing the use of a reusable digital ID of an individual if more than 5 years have elapsed since the digital ID was generated. Subrules 5.4(2) and 5.4(3) provide exceptions to the prohibition in subrule 5.4(1).

5.15 Subrules 5.4(2) and (3) set out the different identity proofing processes that must be completed depending on the IP level of the digital ID, so the digital ID does not "expire" within 5 years of an event. Generally, a digital ID must not be used 5 years after the date the digital ID was first generated, if a document or other credential has not been verified since that time, or biometric binding has not been completed since that time, depending on the relevant IP level for the digital ID.

5.16 Upon commencement of the Rules, accredited entities subject to this obligation are required to comply with this rule, including in relation to a reusable digital ID that was generated before the commencement of the Rules pursuant to subrule 5.4(4). This means that a transitioned accredited entity who is an ISP that has digital IDs that were created and operated under the TDIF pilot accreditation program, would fall under this rule; and the 5-year time period is taken to have started when that digital ID was first generated. The effect of this rule is that, for example, an IP2 digital ID, created on 17 September 2022, will expire on 16 September 2027, unless

that digital ID has been updated (such as when an individual verifies a document or credential) in accordance with subrule 5.4(2)).

5.17 By setting a maximum period after which information in an individual's digital ID should be re-verified, the intention of this rule is to ensure that an individual's digital ID and their personal information remains current to mitigate digital ID fraud and cyber security risks. This is important for the accuracy, reliability and relevancy of the information associated with the digital ID, including where a relying party seeks assurance that the information is accurate.

5.18 This rule sets a maximum time period and does not limit an ISP from maintaining shorter timeframes to verify information in accordance with subrule 5.4(2) or (3), or to stop the use of a digital ID prior to 5 years passing, taking into consideration digital ID fraud risks and cyber security risks associated with the retention of an individual's personal information.

Rule 5.5 Step-up of an identity proofing level

5.19 Subrule 5.5(1) prescribes the circumstances in which an ISP may "step-up" or increase the IP level for an individual's reuseable digital ID. The circumstances in subrule 5.5(1) must be met for an ISP to step-up the IP level. The purpose of this rule is to ensure that an ISP does not step-up an individual's reusable digital ID without first ensuring that the higher-level digital ID meets the appropriate authentication requirements. This is to maintain the security posture and manage the digital ID fraud risks associated with authenticator compromise of a digital ID.

5.20 For example, if an individual has set up a digital ID at IP1 and AL1 (essentially just a username and password) and wants to step up that digital ID to IP3, this rule requires the individual's digital ID to first satisfy AL2 requirements. After that, the individual must authenticate at the higher AL to their existing digital ID prior to finishing the identity proofing for IP3. This mitigates the risk of digital ID takeover or compromise in a scenario where an individual has completed the IP3 identity proofing process, but the authentication level is still at AL1, meaning that the digital ID is vulnerable to authentication compromise.

5.21 Subrule 5.5(2) requires an ISP to notify the individual of the new IP level bound to their digital ID when step-up is completed.

Rule 5.6 Updating and correcting attributes

5.22 Subrule 5.6(1) prescribes that ISPs must allow an individual to update or correct an attribute that the ISP has bound to the individual's digital ID. For example, where an individual has changed their name and wishes to update that information bound to their digital ID, the ISP must allow the individual to do so. The intention of this rule is to complement APP 10, APP 12 and APP 13 to ensure that an individual's personal information remains up-to-date, accurate and complete, and that an individual has access to update that information and correct it, should that be necessary.

5.23 Subrule 5.6(2) sets out the actions that an ISP must undertake before binding the updated or corrected attribute.

5.24 Subrule 5.6(3) sets out the actions that an ISP must undertake if the individual's names or date of birth are not consistent across documents or other credentials. This

requirement is an important digital ID fraud mitigation measure and also supports subrule 5.6(1) above, ensuring that information is up-to-date, accurate, complete, and not misleading to relying parties who may receive that information as part of a digital ID transaction. This rule is limited to an individual's given name, family name and date of birth due to the broad variances in issuance processes for documents and credentials that list additional names, including middle names. Where an individual has additional names, such as middle names, an ISP may consider how checking for matches for middle names across documents can assist with its obligations to mitigate Digital ID fraud risks.

Rule 5.7 Suspending the use of a digital ID

5.25 This rule prescribes the requirements for an ISP if an individual requests that the ISP temporarily suspend their digital ID. Suspension of a digital ID can be considered as a type of "pause" on the use of the digital ID and can be requested by an individual under this provision, and is required in relation to a digital ID affected by a fraud or cyber security incident covered by rule 5.8.

5.26 Paragraphs 5.7(a) and (b) provide that an ISP must confirm the legitimacy of any request to suspend a digital ID and, as soon as possible after the confirmation, suspend the use of the digital ID. This rule does not set a timeframe for suspension and each ISP may determine the appropriate period of suspension.

5.27 An example of when an individual might want to suspend their digital ID is where they are leaving Australia for an extended period and want to reduce the risk of their digital ID being compromised while they are overseas. In such cases, the ISP must only take action to suspend the digital ID after confirming the request is legitimate. For example, the ISP might request that the individual verifies their ownership of the digital ID by having the individual re-authenticate to their digital ID, confirming details of recent usage events or confirming which credentials have been verified as part of the identity proofing process and when they were verified.

5.28 Paragraph 5.7(c) also requires the ISP to inform the individual of the suspension and the process to resume their digital ID.

Rule 5.8 Digital IDs affected by a fraud or cyber security incident

5.29 This rule prescribes the actions that an ISP must undertake in response to a suspected digital ID fraud incident or suspected cyber security incident, including when the ISP must suspend the digital ID.

5.30 In particular, paragraph 5.8(1)(b) relevantly requires the ISP to take reasonable steps to confirm that the individual has effective control of their digital ID. For example, this could be done by requiring the individual presenting the digital ID to successfully pass additional challenge prompts that are suitable to validate that the presenting party is indeed the individual associated with the digital ID. The challenge prompts may, if the ISP supports it, relate to presentation of a secondary authenticator that was previously bound to the digital ID to facilitate recovery processes.

5.31 Paragraph 5.8(1)(c) and subrule 5.8(2) have the effect of requiring an ISP to suspend the digital ID where the ISP is unable to confirm that the individual has effective control of their digital ID, or the ISP suspects that the digital ID has been, or is likely

to be, compromised due to a digital ID fraud incident or a cyber security incident.

5.32 Requirements relating to resuming a suspended digital ID are set out at rule 5.9.

Rule 5.9 Resuming the use of a digital ID

5.33 This rule sets out the steps that an ISP must take when resuming the use a suspended digital ID.

5.34 Subrule 5.9(1) provides for the requirements an ISP must follow for resuming the use of a digital ID suspended in accordance with rule 5.7, which relates to temporary suspension at the individual's request.

5.35 Subrule 5.9(2) provides for resuming a digital ID suspended in accordance with subrule 5.8(1), which relates to suspension of the use of a digital ID because of a cyber security incident or digital ID fraud incident. Subrule 5.9(2) does not require an ISP to resume the use of the digital ID that was suspended due to a fraud or cyber security incident. However, where the ISP does resume the use of the suspended digital ID, the ISP must ensure that the individual completes identity proofing at the level of the suspended digital ID.

5.36 As a matter of policy, ISPs are encouraged to consider implementing a process to resume digital IDs suspended due to digital ID fraud incident or cyber security incident, including best practice remediation and support processes for individuals affected by a digital ID fraud or cyber incident, particularly where a digital ID may have been suspended by the ISP in error. Where an ISP does not implement a process to allow an individual to resume the use of a digital ID suspended due to a fraud or cyber security incident, an ISP should consider usability or accessibility risks associated with requiring an individual to create a new digital ID, should that individual wish to continue using the ISP's accredited services.

5.37 For example, a digital ID may have been suspended due to the ISP's fraud detection mechanisms flagging suspicious activity and the ISP was not able to confirm whether the individual had effective control of their digital ID at the time. The ISP may later confirm that the activity was legitimate, and the digital ID was not compromised. Control of the digital ID may therefore be restored to that individual. This process is comparable to processes used by banking institutions in respect of suspending the use of credit cards when suspicious transactions are identified.

5.38 Subrule 5.9(3) relevantly provides that an ISP is not required to resume a suspended digital ID where the ISP no longer holds the information that would enable it to do so. The purpose of this subrule is to recognise that certain ISP architectures may not allow the ISP to compare the attributes received as part of the re-proofing process against the attributes bound to the suspended digital ID. This may occur where, for example, the period of suspension may have stretched beyond the ISP's data retention policies for digital IDs that have been suspended without action from the individual to resume the use of the digital ID. Therefore, the ISP may consider that it is appropriate to destroy the personal information held for that digital ID in order to mitigate cyber security risks or comply with other legislative obligations associated with the retention of that information.

5.39 Additionally, this rule recognises scenarios where a digital ID was generated fraudulently from the outset (i.e. a malicious actor purchased an individual's ID documents online and had them verified before they were cancelled, thus generating

a seemingly legitimate digital ID). Without knowing or having the legitimate individual's details, or the individual's consent for the generation of that digital ID, the ISP may delete the personal information used to generate the fraudulent digital ID. In this way, while suspension should be the first action ISPs take in response to a fraud or cyber incident, the ISP may decide to not resume a digital ID if, for example, they know the legitimate individual doesn't want a digital ID, or the ISP wants to minimise risks related to data retention and therefore destroy the personal information that would be required to resume the digital ID.

Division 2—Identity proofing and use of credentials

Subdivision A—Identity proofing

5.40 This Subdivision sets out rules that relate to minimum requirements for the identity proofing of individuals at different levels of assurance. The identity proofing process involves verifying information contained on or within one or more presented credentials or documents listed at Schedules 1 to 4 of the Rules. Additional requirements for other processes such as biometric binding apply at higher IP levels to increase the assurance of the individual's digital ID. ISPs must also comply with accessibility and useability rules that relate to the proofing process in Division 4 of Part 5.1 to this Chapter.

Rule 5.10 IP Levels Table

5.41 Rule 5.10 and the table under subrule 5.10(2) provides for the IP Levels Table. Broadly, the IP Levels Table specifies 6 different IP levels and the minimum requirements for each IP level. The table does not restrict an ISP from applying, for a particular IP level, the requirements for a higher proofing level (subject to the entity's accreditation conditions). This allows, for example, an ISP to conduct a biometric binding check at lower IP levels as a fraud mitigation measure, provided the ISP has a condition on its accreditation. However, it does not enable an ISP that applies elements of a higher proofing level, beyond the scope of its accreditation, to claim that its accredited service offers digital IDs at the higher IP level as per subrule 5.10(2).

5.42 For example, an ISP may choose to apply more stringent binding approaches that apply biometric techniques such as PAD technology and liveness detection, but only if the ISP has been explicitly authorised to collect biometric information as a condition of their accreditation. Primarily, these requirements exist to provide ISPs with options to generate digital IDs for a range of use cases, from low-risk (IP1 - low assurance) to high-risk (IP4 - very high assurance) scenarios. Generally, generating an IP1 digital ID only requires few checks, and increasing types and sophistication of checks are required for increasing IP levels. The higher an IP level, the greater the level of trust and assurance a relying party and the ISP can have that the individual using a digital ID is who they say they are.

5.43 **IP1** is used when no verification of the individual's identity is needed, or when a very low level of confidence is needed in the claimed identity. IP1 supports a self-asserted identity ('this is me') or a pseudonymous identity, with no verification of documents or credentials required.

5.44 **IP1 Plus** provides low confidence in the claimed identity. IP1 plus requires verification of name and date of birth details contained in one (or more) documents or credentials, at least including either a UitC credential or a photo ID.

5.45 **IP2** provides low-medium confidence in the claimed identity. It requires verification of name and date of birth details across 2 (or more) documents or credentials, one of which must be a UitC credential.

5.46 **IP2 Plus** provides a medium level of confidence in the claimed identity. It requires verification of name and date of birth details across 2 (or more) documents or credentials and additionally requires biometric binding to reliably verify the link between the individual and the claimed identity.

5.47 **IP3** provides high confidence in the claimed identity. It requires verification of name and date of birth details across 3 or more documents or credentials and additionally requires biometric binding to reliably verify the link between the individual and the claimed identity.

5.48 **IP4** provides very high confidence in the claimed identity. It requires verification of name and date of birth details across 4 or more documents or credentials and additionally requires biometric binding to reliably verify the link between the individual and the claimed identity.

5.49 Each rule in Division 2 of Part 5.1 to this Chapter relates to meeting the requirements of the IP Levels Table in some way.

5.50 Within the IP Levels Table, each row is assigned an item number reference. Each of the 14 items relates to a requirement that must or in some cases is recommended to be met in proofing an individual's identity. The number of applicable requirements increases according to the IP level. The items are broadly explained below.

- **Item 1** requires that a digital ID identifier chosen by the individual must be unique. Examples include individually chosen identifiers such as 'account name', 'username' or 'email address' when used to identify a specific digital ID.
- **Item 2** concerns the ISP checking to establish that the identity is unique. As it is possible for an individual to maintain a digital ID with multiple ISPs, this check need only focus on the ISP's own information holdings to, for example, confirm that the set of presented attributes is not already associated with an existing digital ID.
- **Item 3** concerns confirming the identity does not belong to an individual who is deceased. While this is not a mandatory requirement for levels below IP3, certain authoritative sources such as the DVS do incorporate updates to some documents or credentials in relation to the death of an individual and may return a negative match result if the presented document or credential details are recorded as belonging to a deceased person.
- **Item 4** concerns identity proofing through biometric binding. The rules concerning biometric binding are located at Subdivision B.
- **Item 5** concerns a requirement for original documents or credentials to be presented and verified in-person. This is only applicable for identity proofing to IP4.

- **Item 6** concerns a requirement that identity details be checked against information or records held by the ISP to confirm whether the identity has been previously associated with fraudulent activity, such as a blocklist of known fraudulent identities.
- **Item 7** provides that the personnel undertaking identity proofing processes, including visual verification, are required to be provided with tools and training to detect fraudulent attributes, documents or other credentials, before starting work on these duties and annually thereafter.
    - In effect, if an ISP supports manual identity proofing processes (such as in-person presentation at a shopfront) then all persons who conduct in-person identity proofing processes must be trained and provided tools to aid detection of fraudulent credentials (such as a falsified birth certificate) or fraudulent attributes (such as altering the date of birth shown on an otherwise valid driver's license). Such training is to be provided prior to commencement of duties and annually thereafter.
- **Item 8** concerns the need to employ accredited translators to translate documents or credentials that are not in English.
- **Item 9** identifies the attributes that must be verified by source verification or technical verification. This requires one or more of the presented credentials to list both the individual's date of birth, and relevant names. Verification may be performed using either source verification (as described by rule 5.14) or technical verification (as described by rule 5.15)
- **Items 10, 11, 12** are concerned with the verification of various credentials to achieve each IP level. For example, proofing at IP1 Plus requires verification of a single credential, either a photo ID or a UitC credential; while proofing at IP2 requires verification of 2 credentials, one being either a photo ID or a CoI credential and the other being a UitC credential. Acceptable credentials in each category are listed in Schedule 1-4 of the Rules.
- **Item 13** broadly requires an ISP to verify a linking credential if an individual's given name, family name or date of birth varies across documents or other credentials. This rule is limited to an individual's given name, family name and date of birth due to the broad variances in issuance processes for documents and credentials that list additional names, including middle names. Where an individual has additional names, such as middle names, an ISP may consider how checking for matches for middle names across documents can assist with its obligations to mitigate Digital ID fraud risks.
- **Item 14** identifies the approved ALs to which a digital ID may be bound. Details of the requirements to be met at each AL are included in the AL Table within the Accreditation Data Standards.

Rule 5.11 Verification using an Australian passport

5.51 Subrule 5.11(1) relevantly provides that for Items 10 and 11 in the IP Level Table, if an Australian passport is being used for IP3, it can also be used to simultaneously meet the CoI credential and photo ID requirements.

5.52 Subrule 5.11(2) relevantly provides for Item 10 in the IP Levels Table, if an Australian passport is being used for IP4, it can be used to meet either the CoI credential or the photo ID requirement for IP4, but not both.

5.53 Australian passports have well-established eligibility and issuance requirements that generally exceed other types of government-issued identity documents. This includes requirements concerning the capture and display of an individual's biometric information that can be used to satisfy the verification and biometric matching rules for a photo ID at IP3. An Australian passport can be used as a CoI credential because its issuance process requires that a birth certificate, which is a CoI credential, is checked. Because of the level of trust in this kind of document, Australian passports can be used to meet 2 kinds of credential types (where usually 2 distinct identity documents would be required) specifically at IP3. However, this does not apply to IP4, which aims to apply the most rigorous checks of all IP levels. Requiring individual documents for each category results in greater assurance, as successfully creating more types of fraudulent identity documents that pass verification checks is considered to be an increased challenge for fraudsters.

Rule 5.12 Technical verification of credentials

5.54 This rule sets out the requirements that apply if an ISP uses technical verification to verify an Australian passport or a foreign ePassport (referred in this section collectively as "ePassports").

5.55 Technical verification refers to validating specific kinds of documents that have built-in cryptographic elements that can be checked for:

- authenticity, which is about whether the document was created by the issuing authority for that document type; and
- integrity, which is about whether the information has been altered since being placed on the document by the issuing authority.

5.56 This rule provides for the requirements relevant to an ISP when performing verification of an ePassport via public key infrastructure (PKI) technology, using approved cryptographic protocols and algorithms.

5.57 Technical verification is commonly performed to verify ePassport attributes by using Near Field Technology (NFC) to scan the contactless integrated circuit—a kind of chip that uses Radio frequency identification (RFID) technology— embedded in the ePassport, and verifying digital signatures on the scanned data to confirm it is authentic and has not been modified.

5.58 ePassports are designed to meet the internationally agreed standards for biometric travel documents agreed and set out by the ICAO. The ICAO Standards ensure that biometric travel documents are secure and work across border systems globally. This rule requires that ICAO Doc 9303 Standard, which sets out the design, issuance and verification standards for ePassports, is adhered to when verifying an ePassport, and expressly requires that the verification includes a step to confirm that the ePassport has not been revoked.

5.59 The assurance that a technical verification check can provide comes from checking elements of the identity document in the possession of the user. For this reason, only documents with a range of security features, and that have trusted standards for how

to verify that document, can be used for technical verification.

5.60 Upon commencement of the Rules, the only kind of document allowed to be verified using technical verification are valid ePassports. This is because the ICAO Doc 9303 Standard is available as an international and agreed upon standard of issuance for this type of document and has well-established mechanisms for certificate validation and PKI. Additionally, ePassport chips are very difficult to clone (i.e., duplicate a genuine chip) or alter (i.e., change the biographic or biometric information stored on the chip), and as such, can be relied upon to provide a meaningful amount of assurance.

Rule 5.13 Source verification using non-government credentials

5.61 This rule sets out the requirements applicable to an ISP if it uses a document, or other credentials issued by a non-government entity for verification purposes.

5.62 An example document type that is non-government issued would be a debit or credit card.

5.63 Generally, source verification systems for government-issued documents or credentials have well-documented protocols for how to connect and verify documents or credentials using that authoritative source. This rule re-creates some features of this assurance for non-government credential sources to ensure the integrity and security of the verification process.

Rule 5.14 Visual verification

5.64 This rule prescribes the requirements for an ISP in relation to ***visual verification*** of a document or other credential. The term visual verification is defined in rule 1.4 and may include, for example, having a trained member of personnel inspect a Veteran Card for holograms, fine printing, or the expected layers in the document construction. Being able to perform this check with a high degree of consistency and reliability involves training to understand what security features are available to look for and common methods malicious actors use to create or modify fraudulent documents.

5.65 This rule broadly requires that visual verification must be conducted by an appropriately trained person and visual verification should not be conducted if the results of a source verification or technical verification indicates that the document or credential is not legitimate. This is because verifying documents or credential information with the authoritative source or verifying information using cryptographic processes are generally considered to be stronger fraud mitigation processes than visually inspecting a document. That is, creating or modifying a physical document that could fool a person is considered easier than fooling an authoritative source, or modifying or cloning the RFID chip of an ePassport.

Subdivision B—Verification using biometric information

Rule 5.15 Application

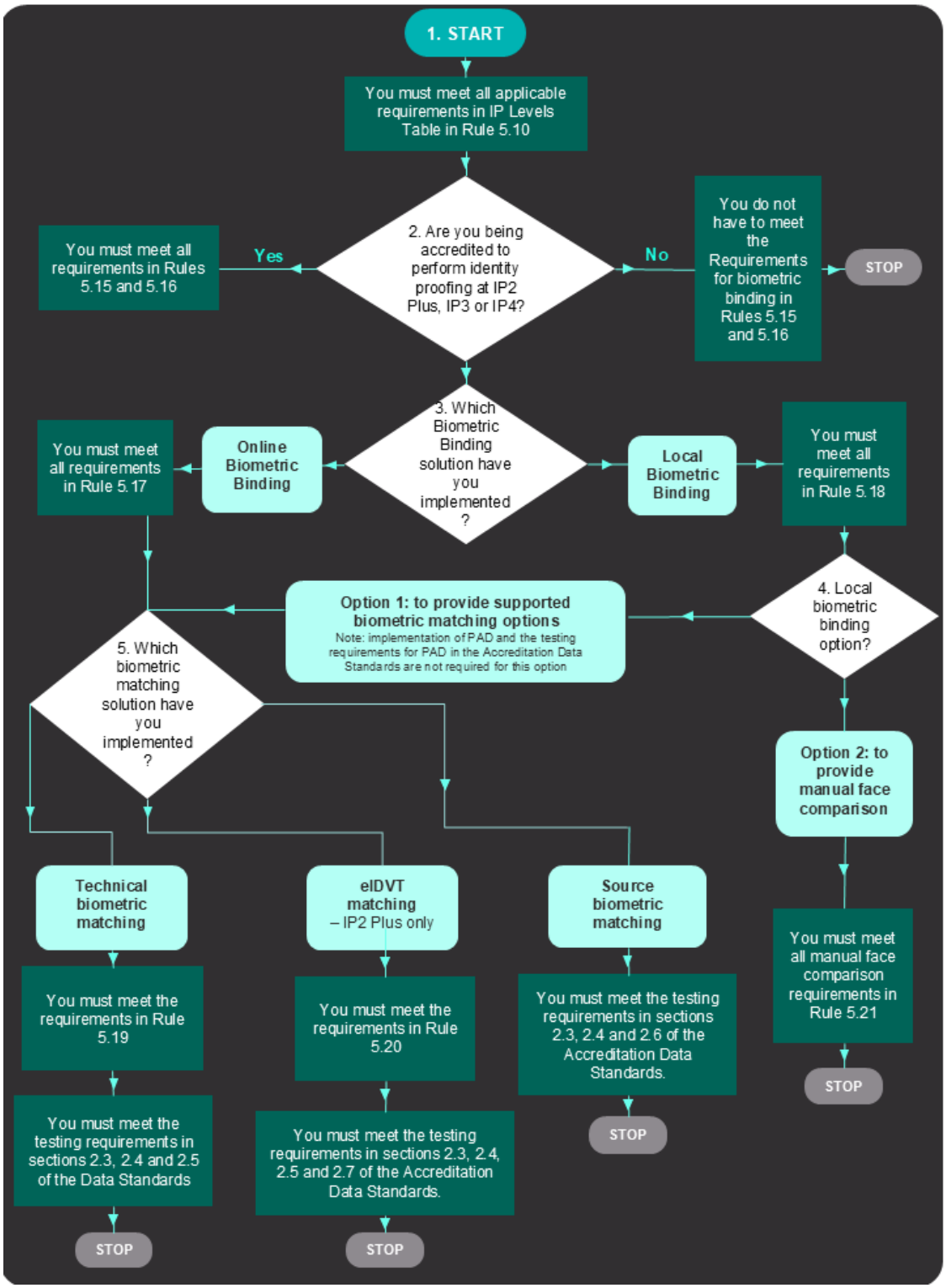
5.66 This rule provides for the application of this Subdivision, which is to ISPs conducting identity proofing at IP2 Plus, IP3, and IP4; and for the requirements for

biometric binding options to achieve those IP levels. Biometric binding checks the link between the individual and the claimed identity.

5.67 Verification using biometric information requires an individual to provide a biometric sample such as an image of their face, and for the ISP to match that sample against a trusted reference, which is the image associated with a photo ID. These rules exist to increase the consistency, reliability, and quality of this process.

5.68 The following flow chart describes which requirements in this Subdivision apply to an accredited entity depending on which biometric binding solution it implements. It is provided as a visual representation to assist readers.

Figure 1 – ISP Biometric binding requirements applicability flowchart



Rule 5.16 Requirements for biometric binding

5.69 This rule prescribes that biometric binding may be conducted either using online biometric binding, which is set out in rule 5.17, or local biometric binding, set out in rule 5.18.

5.70 Biometric binding can occur in 2 distinct contexts: either in person (for example, at a service centre or shopfront facilitated by an ISP's assessing officer) or online (where an individual independently uses their smartphone or other device connected to the internet).

5.71 Differences in the rules for these 2 types of biometric binding are largely driven by the fact that local biometric binding is supervised, and online biometric binding is unsupervised. Because local biometric binding is facilitated by a physically present assessing officer, this pathway is more flexible in the kinds of evidence types that can be accepted, for example, documents that do not have cryptographically verifiable evidence. Additionally, local biometric binding is generally more suitable for vulnerable cohorts or individuals who may need assistance to complete the biometric binding process and may be more flexible to support alternative proofing methods (where required).

5.72 ISPs can choose whichever pathway, online or local biometric binding, that suits the configuration of their accredited services.

5.73 Regardless of the biometric binding approach used, subrule 5.16(2) requires that the ISP verifies a photo ID using source verification before starting the biometric binding process.

5.74 Subrule 5.16(3) prescribes that if the photo ID presented for biometric binding is a foreign passport, the ISP must also ensure that the passport must be linked to an Australian visa that has been source verified, and the biometric binding process must not be conducted until the linking of the visa and passport is verified. This is to ensure that the CoI credential verification requirement is achieved prior to conducting the biometric binding process, which will ensure that the individual meets other eligibility identity proofing requirements for a digital ID.

Rule 5.17 Requirements for online biometric binding

5.75 This rule prescribes the requirements for ISPs when performing online biometric binding.

5.76 Broadly, it includes requirements for:

- the acceptable biometric matching options to be used for online biometric binding (subrule 5.17(1)), and
- quality controls and other requirements for biometric information captured during the biometric binding process (***acquired image***) (subrules 5.17(2) to (5)), and
- fraud and security controls related to implementing PAD technology and liveness detection to identify if a presenting individual is attempting to subvert the intended function of biometric matching technologies (subrule 5.17(6)).

5.77 Subrule 5.17(1) sets out the acceptable biometric matching options to be used to conduct online biometric binding. Each biometric matching option includes a process for conducting the biometric match as set out in the Rules. Testing requirements for each biometric matching option are set out in the Accreditation Data Standards.

General process for online biometric matching

5.78 Generally, the process of online biometric binding is to match a trusted image that an individual has taken of themselves (i.e. a "selfie") against a trusted reference biometric image. This involves a process to:

1. Acquire a selfie image from an individual and ensure:
    a. the image is of high enough quality for biometric matching (by ensuring it passes a biometric quality threshold), and
    b. the image can be trusted as a genuine image of that individual (by ensuring it passes PAD and liveness detection).
2. Identify or extract a trusted reference image that is known to be of the identity associated with a presented photo ID (how this image is obtained or identified is dependent on the type of biometric matching process and photo ID used).
3. Perform (or facilitate) a biometric match between the selfie and the trusted image or biometric representations thereof (this process is dependent on the type of biometric matching process used).

5.79 If the images match, then the biometric binding requirement in Item 4 of the IP Levels Table is met.

Pathways for biometric matching

5.80 Differences between online biometric binding types relate to how or where the trusted reference biometric image for a photo ID is sourced.

- For **source biometric matching:** the image is held in a central identity matching system, often managed by the issuing authority for the photo ID—the authoritative source.
- For **technical biometric matching:** the image is securely stored on the document's cryptographically verifiable evidence (e.g. the RFID chip on an ePassport).
- For **eIDVT matching:** the image is physically printed on a photo ID (e.g. the facial image on a driver licence).

5.81 Despite these differences, each type of biometric matching solution conducted using online biometric binding requires the use of PAD and biometric image quality algorithms. ISPs also need to implement and manage a biometric matching algorithm unless they intend to solely use source biometric matching, in which case, the biometric matching is wholly managed by the authoritative source for those images.

Acquired image quality

5.82 Subrules 5.17(2), (3), (4) and (5) relate to the quality specifications and thresholds that are to be developed and applied to an acquired image used for online biometric binding.

5.83 These subrules seek to ensure that acquired images used for biometric matching meet a quality threshold that minimises identity fraud and cyber security risks before submitting that image to PAD technology and a biometric matching algorithm. Image quality is one of the most influential factors in achieving an accurate biometric matching outcome. Higher resolution, consistent poses, and better lighting conditions all supply more data to the biometric matching algorithm, leading to a more precise result.

5.84 The ISO/IEC standard for biometric quality algorithms (ISO/IEC 29794-5) provides a set of characteristics that an image quality profile should consider. These characteristics are qualitative, and do not provide an objective measure like other ISO/IEC standards (e.g. biometric testing standards). Additionally, biometric quality is hugely dependent on use context, with no one type or approach to assessing quality being objectively best. However, because of its importance, ISPs do need to set sensible thresholds for biometric quality to ensure that downstream matching processes are reliable. Any such system should reject images that have poor lighting, posing, or have low resolution. Since the individual can have a direct influence on the photo of themselves being taken, the ISP can achieve good quality and user experience by providing clear real-time prompts to help users take a good quality image.

Presentation attack detection and continuous workflow

5.85 Paragraph 5.17(6)(a) relevantly requires biometric binding to be completed in a continuous workflow as a security and anti-fraud measure. This helps mitigate the risk of insertion attacks (where an attacker provides one image to pass PAD, and another image for biometric matching), and other attacks that compromise the biometric sensor.

5.86 Paragraphs 5.17(6)(b) through to (e) prescribe the process and requirements for the use of PAD, and liveness detection at the point where the ISP captures the acquired image to be used in biometric binding. The use of PAD and liveness detection are anti-fraud measures to ensure that biometric systems cannot be easily compromised and have a robust fraud detection system that indicates a high level of assurance as required at IP 2 Plus and above.

5.87 A biometric presentation attack refers to using a human or artificial device impersonating the qualities of a legitimate biometric to manipulate or fool a biometric system in some way. For example, wearing a latex mask to look like someone else, or generating a convincing deepfake. PAD provides resistance against these kinds of attacks. A reliable and effective PAD system is a critical component for a robust biometric system—even if a biometric system has a tested false match rate of zero, it still may be subject to novel presentation attacks. ISO/IEC 30107-1 provides key characteristics that compliant PAD systems must have and is the industry standard for this kind of technology. Liveness detection refers to a check that the person in the acquired image or images (if it is a video) is alive and not, for example, an AI generated deep fake image that has been injected into the entity's biometric subsystem.

5.88 Accredited entities should consider these requirements in conjunction with the

testing requirements for PAD technology used for online biometric binding, which set out the minimum test standards for that technology to meet before the entity can be accredited, as specified in the Accreditation Data Standards.

Rule 5.18 Requirements for local biometric binding

5.89 This rule prescribes requirements for ISPs when performing local biometric binding.

5.90 Local biometric binding is generally used in an in-person transaction to verify the link between a presenting individual and their claimed identity. Local binding is an approach to biometric binding that must be performed face to face, with the individual presenting in-person to the ISP's assessing officer and providing their physical photo ID to be used in the biometric matching process. Local biometric binding affords ISPs further accessibility and inclusion options for their services, if they wish to leverage the use of shopfronts to assist individuals to create or update their digital IDs.

5.91 A feature of local biometric binding is the presence of an assessing officer. An assessing officer can replace the need for PAD technology, as physical presence can be used as an effective proxy for this—an attacker should not be able to perform presentation attacks without detection in the presence of a trained and experienced assessing officer.

5.92 Subrule 5.18(1) relevantly provides for the acceptable biometric matching processes to be used for local biometric binding and requires that the binding is conducted by an assessing officer in the physical presence of the individual. The intended effect of paragraph 5.18(1)(c) is to restrict the use of eIDVT to biometric binding at IP2 Plus only.

5.93 Subrule 5.18(2) allows the use of manual face comparison as an alternative biometric matching process to those set out in subrule 5.18(1), where those processes are unavailable to the ISP for a kind of photo ID. This is because evidence suggests that biometric matching algorithms are more reliable for conducting identity verification than most humans. This is especially true in the service centre scenario where an assessing officer will be making a visual inspection of the photo ID, manually comparing this to the individual in front of them and deciding whether the individual matches the image on the photo ID (as per manual face comparison).

5.94 If technology-based approaches are not available to the ISP for a type of photo ID (i.e. technical biometric matching, source biometric matching, or eIDVT biometric matching), the assessing officer can perform key roles that would otherwise be performed by technology. This includes:

- performing manual face comparison (rather than using a biometric matching algorithm), and
- inspecting an identity document for authenticity and integrity (rather than using an eIDVT algorithm).

5.95 Subrule 5.18(4) broadly requires that, for an acquired image captured as part of local biometric binding, an image quality profile must be developed and applied in accordance with rule 5.17.

5.96 Subrules 5.18(3) and (5) broadly set out security and fraud mitigation requirements

for the location and conduct of assessing officers involved in the process of local biometric binding.

Rule 5.19 Requirements for technical biometric matching

5.97 This rule prescribes requirements for ISPs when performing technical biometric matching.

5.98 Subrule 5.19(1) relevantly provides that technical biometric matching of an acquired image must only be conducted using an Australian passport or foreign ePassport if that passport has been verified using technical verification in accordance with rule 5.12. Subrule 5.19(2) provides for when a biometric matching algorithm can be used.

5.99 Within the context of biometric binding, technical biometric matching refers to a process by which an ISP may:

- first conduct technical verification of the ePassport by using NFC to scan the contactless integrated circuit—a kind of chip that uses RFID technology—embedded in the ePassport document,
- then verify digital signatures on the scanned data to confirm it is authentic and has not been modified,
- then extract the verified biometric image stored on the RFID chip of an ePassport, and
- finally, use that verified image for biometric matching with the individual's selfie (i.e. the acquired image).

5.100 ISPs should consider these requirements in conjunction with the testing requirements, as specified in the Accreditation Data Standards, for biometric matching algorithms used as part of technical biometric matching and eIDVT processes.

Rule 5.20 eIDVT biometric matching

5.101 This rule prescribes requirements for ISPs when using ***eIDVT*** to perform biometric matching. Pursuant to paragraphs 5.17(1)(c) and 5.18(1)(c), eIDVT is restricted to biometric binding for IP2 Plus only. This is because, unlike source or technical biometric matching, eIDVT does not provide cryptographic or authoritative source evidence that the photo ID being used for biometric binding has not been tampered with. This provision and the requirements in the Accreditation Data Standards related to independently testing the veracity of the eIDVT's ability to detect fraudulent or tampered with documents, provide a high degree of assurance to the Digital ID Regulator and relying parties that the entity's eIDVT works. However, at the time of commencement of the Rules, eIDVT and the testing standards are still relatively new technology, and as such, have been limited to use at IP2 Plus.

5.102 eIDVT refers to the process of using techniques other than technical verification (i.e., non-cryptographic), such as computer vision and machine learning techniques, to detect document fraud or alteration, particularly with reference to ensuring the integrity of the facial image on the claimed photo ID. In general terms, this means using a trained AI algorithm to assess an image or a video feed of an identity

document to determine if it is genuine (i.e., unaltered, issued by a trusted source, etc). If the document is classified as genuine, then the facial image contained within can be used for biometric matching.

5.103 Subrule 5.20(1) relevantly provides for eIDVT biometric matching to only be used for one of the following types of photo IDs:

- a State or Territory driver's licence;
- a State or Territory proof-of-age card;
- an Australian passport.

5.104 This subrule also requires individuals to physically present those photo IDs to a biometric sensor at the time the matching is being conducted.

5.105 These credentials are considered appropriate for eIDVT biometric matching because they can be widely obtained by individuals in Australia but are not widely available to use with other biometric matching technologies (such as source biometric matching or technical biometric matching).

5.106 Subrule 5.17(2) referred to above provides that source verification of a photo ID that will be used for biometric binding must be completed before starting the biometric binding process. However, proof-of-age cards have limited options to perform source verification for some organisations.

5.107 Subrule 5.20(2) sets out the controls for eIDVT to meet to determine that a physically presented document is authentic and has not been tampered with. This includes the use of document liveness technology to determine that the physical document is in the presence of the biometric sensor and a range of checks to ensure that the document is not, for example, a copy or a generated image injected into the entity's eIDVT designed to fool it into thinking a legitimate document is present.

5.108 Subrule 5.20(3) prescribes the controls for the effective use of ***Optical Character Recognition (OCR)*** technology for eIDVT. OCR technology automatically converts and sorts text on a document into relevant text fields (e.g. first name, last name, driver's licence number). OCR is required to be used by the eIDVT and does not allow manual human review processes to ensure that the OCR lifted text on the credential matches that of the credential that has been source verified. This is to prevent attackers from changing or tampering with information on a legitimate document after it has been verified using source verification but before the biometric match has been carried out.

5.109 Additionally, OCR technology helps ensure that any other information on the document that is captured by the ISP but is not able to be verified by an authoritative source is accurate (e.g. some fields may not be available to be matched, such as an individual's address).

5.110 Subrule 5.20(4) sets out the core criteria for a photo ID before it can be processed through eIDVT. Subrule 5.20(5) relevantly prescribes matters which the ISP must confirm when processing a photo ID through eIDVT. The purpose of an eIDVT algorithm is to assess the authenticity and integrity of a presented photo ID. This includes checking for the expected visual security features that should be present for that kind of document. This could include:

- Guilloche

- Holographic laminate
- Laser engravings
- Microprint
- Clear windows
- Relief embossing
- Secondary photos

5.111 Subrule 5.20(6) defines ***identity document template*** for the purposes of this rule.

5.112 Using an established identity document template—which is a model representation of a particular type of identity document—enables ISPs to compare a presented document with its expected formatting, colouring, text alignments, as well as the aforementioned security features. eIDVTs can also consider other information to check for consistency (for example, dates of birth, consistency of spelling, placement and alignments of text). In addition to checking formatting and colouring, this can include the text information, read using OCR.

5.113 Subrule 5.20(7) sets out requirements for an ISP after they have processed the photo IDs through eIDVT. Generally, an ISP must destroy any images (including copies) of the photo ID that has been processed as genuine through the entity's eIDVT. However, the ISP may retain images of photo IDs in accordance with the requirements concerning biometric information retention for fraud purposes under the Digital ID Act. In particular, ISPs may retain images of photo IDs that have been classified as being fraudulent for up to 14 days. This not only aids investigations into potential cases of fraud, but also assists in providing insight into common or emerging attack vectors for the creation or alteration of fraudulent identity documents.

5.114 Subrule 5.20(8) prohibits an ISP from using a facial image acquired from a photo ID for eIDVT biometric matching unless the criteria set out in this subrule are met.

5.115 This rule relevantly applies image quality profile requirements for the image on the photo ID to help ensure that an accurate biometric match can be carried out. If, for example, the image on the document has been scratched or damaged, the image on the document, even if classed as genuine by the eIDVT, may not provide enough detail to give assurance that the biometric match can be carried out.

5.116 Subrule 5.20(9) requires an ISP to use a biometric matching algorithm to perform a one-to-one match between the individual's acquired image (i.e. selfie) and the acquired facial image from the photo ID.

5.117 The eIDVT requirements set out in the Rules operate in conjunction with the requirements set out in the Accreditation Data Standards, including the testing standards for eIDVT and the entity's biometric matching algorithm.

5.118 Subrule 5.20(10) requires an ISP to ensure that verification, identification and detection processes do not result in any damage to the photo ID being processed.

5.119 In practice, the process for online biometric binding using eIDVT as the biometric matching process generally includes the following steps:

1. The user takes photo (or video) of their eligible photo ID.

2. The ISP system uses an eIDVT to analyse the captured photo (or video) for authenticity by checking for presence of security features, checking for evidence of tampering, etc.
3. If the eIDVT returns a positive result, the ISP system checks the quality of the biometric sample on the photo ID for sufficient quality (using a compliant biometric quality algorithm).
4. The ISP system prompts the user to capture a selfie and subjects the capture of the selfie to PAD.
5. If the selfie capture passes PAD, the ISP system uses a biometric matching algorithm to compare the selfie with the image scanned from the photo ID.
6. If the match is successful, then the biometric binding objective using eIDVT biometric matching has been met.

Rule 5.21 Requirements for manual face comparison

5.120 This rule prescribes the requirements for manual face comparison.

5.121 Subrule 5.21(1) provides that manual face comparison must be conducted using only an original, physical, photo ID presented in person by the individual at the time the manual face comparison is conducted.

5.122 Subrule 5.21(2) sets out obligations on ISPs in relation to manual face comparisons. These obligations broadly relate to requirements around assessing officers carrying out manual face comparison.

5.123 Generally, manual face comparison can be achieved in a shopfront by an individual presenting a photo ID to an assessing officer, who will perform a manual face comparison between the individual and the image on the photo ID. To be eligible to perform this role, assessing officers must undergo awareness training that aligns to the Facial Identification Scientific Working Group's *Guide for Facial Comparison Awareness Training of Assessors*. In addition to performing source verification of the photo ID (for example, performing a check using the DVS), the assessing officer has the responsibility to check the security features of the presented photo ID (for example, reflective markings on a driver's licence holographic features).

5.124 Paragraph 5.21(2)(d) relevantly requires that an ISP record in its SSP and FCP its procedures in relation to detection of fraudulent activities in relation to manual face comparison decisions made by assessing officers. This is to ensure that the ISP is aware of and mitigates any cyber security or digital ID fraud risks (including corruption) associated with the conduct of assessing officers during the manual face comparison process. For example, any cyber security risks associated with an assessing officer having access to the ISP's biometric capability to make decisions related to the identity proofing outcomes of an individual, or the digital ID fraud risks associated with an assessing officer being able to make determinations as to whether an individual biometrically matches their photo ID.

Subdivision C—Alternative proofing processes

Rule 5.22 Accessible and inclusive services

5.125 This rule provides that this Subdivision applies for the purposes of subsection 30(1) of the Digital ID Act. It sets out alternative proofing processes as a means of ensuring all individuals can obtain a digital ID if they choose to, in situations where the individual does not possess, and is unable to obtain, the documents or other credentials required to generate a digital ID at the particular IP level sought by the individual.

Rule 5.23 Requirements for an alternative proofing process

5.126 This rule details the circumstances in which an ISP can use an alternate identity proofing process for the purpose of establishing a digital ID.

5.127 Subrule 5.23(1) provides that an ISP may only conduct an alternative proofing process if they have been authorised to do so as a condition of their accreditation, and only in the circumstances specified in the conditions.

5.128 Subrule 5.23(2) prescribes a non-exhaustive list of matters which may be included in an alternative proofing process.

5.129 Subrule 5.23(3) sets out the requirements which an ISP must meet before undertaking an alternative proofing process.

5.130 Subrule 5.23(4) defines ***exceptional use cases*** within the context of this rule. An exceptional use case refers to a situation where an individual lacks the necessary documents or other credentials to establish a digital ID at a desired IP level. An example of an exceptional use case could be a child over the age of 15, who cannot present a valid photo ID or does not hold the full set of credentials or documents required to achieve higher IP levels.

5.131 The alternate proofing process is important as it accommodates individuals who cannot provide standard identity documents or credentials due to exceptional circumstances. This rule sets out the different proofing methods which an alternative proofing process may include, such as:

- accepting different types of documents,
- verifying identity through trusted referees or reputable organisations, and
- conducting interviews with the individual.

Division 3—Generating, binding, managing or distributing authenticators

5.132 This Division sets out requirements for the creation, binding, management and distribution of ***authenticators*** that are bound to a digital ID. The definition for authenticator is set out in section 9 of the Digital ID Act and further technical requirements for authenticators to achieve a specified AL1, 2 or 3 are contained in the Accreditation Data Standards.

Rule 5.24 General requirements

5.133 This rule prescribes requirements applicable to all authenticators, including the requirements for authenticators to meet when bound to a digital ID. This rule also references the AL Table.

5.134 This rule prescribes requirements related to events that may occur over the lifecycle of an individual's authenticator that affect that authenticator's use, including where the authenticator is generated, bound to a digital ID, expires, or cannot be used. The intention of this rule is to ensure there are adequate requirements for the ongoing risk management of authenticators that the accredited entity generates, binds, manages or distributes.

Rule 5.25 Physical authenticators

5.135 This rule defines the types of authenticators that can be classified as a ***physical authenticator.***

5.136 A physical authenticator refers to a device or method used to authenticate and verify an individual's identity, based on checking that the individual still possesses something that the individual demonstrated that they possessed at the time of creating the digital ID.

5.137 Subrule 5.25(1) provides the list of physical authenticators.

5.138 Subrule 5.25(2) prescribes requirements for ISPs that conduct authentication using physical authenticators. ISPs that bind digital IDs to a physical authenticator must provide clear instructions to individuals about how to protect the authenticator against theft or loss; and must be able to immediately suspend or revoke use of the physical authenticator in certain circumstances. The capability to suspend an authenticator is distinct from the capability to suspend or deactivate the digital ID that has been bound to the authenticator.

5.139 Characteristics of each type of authenticator and related requirements are set out in the Accreditation Data Standards.

Rule 5.26 Authenticator that has been compromised

5.140 Subrule 5.26(1) defines a ***compromised authenticator*** in the context of rule 5.26 as an authenticator that has been lost, stolen, damaged, or duplicated without authorisation. This subrule also requires an ISP to immediately suspend the use of, revoke or destroy a compromised authenticator.

5.141 Subrule 5.26(2) requires that if an ISP reasonably suspects a transaction involves a digital ID fraud incident or cyber security incident, the ISP must verify that the relevant authenticator has not been compromised. Once an authenticator is compromised, it is no longer considered a legitimate authenticator and must be suspended, revoked or destroyed. Additionally, damaged or malfunctioning authenticators are to be considered compromised, so as to protect against the potential of an authenticator secret being extracted by an attacker.

5.142 These requirements pertain to all forms of physical and software-based authenticators, including hardware tokens, smart cards, authentication apps on mobile, and any linked memorised secrets.

5.143 It is expected that an ISP will take the following actions for each type of authenticator:

- **Hardware Authenticators**: physically destroyed or handed over.
- **Software Authenticators**: Need to be deactivated, uninstalled, or have access revoked.
- **Memorised and Look-up Secrets**: made invalid or changed to prevent unauthorised access.

5.144 The ISP may cease using a physical authenticator as a verifier, which also applies to software-based authenticators on mobile devices. By un-enrolling the device, the ISP can ensure the software authenticator can no longer be used to authenticate the individual's identity because the device is no longer recognised as enrolled.

5.145 Furthermore, disabling the software on an individual's mobile device is a crucial step to secure the device. This action typically involves revoking the software's access or deactivating the associated account. The primary goal of this rule is to prevent unauthorised access and ensure the security of the individual's identity.

5.146 Subrule 5.26(3) allows an individual to authenticate their digital ID using an alternative authenticator to facilitate the secure reporting of a compromised authenticator to the ISP. If they do so, the alternative may only be via a memorized secret or physical authenticator. The purpose of this rule is for the individual to confirm the legitimacy of their report of a compromised authenticator by establishing a secured communications channel to the ISP and by verifying a sample of 'shared secret' identity information that they provided during the identity proofing process.

Rule 5.27 Expired and renewed authenticators

5.147 This rule sets out the requirements for expired and renewed authenticators. As per subrule 5.24(6), an ISP may issue authenticators that expire. Where an ISP does issue such authenticators, it must comply with this rule.

5.148 Subrule 5.27(1) prohibits ISPs from allowing an individual to use an expired authenticator.

5.149 Subrule 5.27(2) relevantly requires an ISP to take appropriate action in relation to the type of authenticator that has expired as soon as practicable after an authenticator expires or a renewed physical authenticator is bound to an individual's digital ID.

5.150 Subrule 5.27(3) provides a non-exhaustive list of matters that may constitute the appropriate actions that an ISP must take to ensure the expired authenticator is not used, which depends on the authenticator type. For example, the ISP may ensure the prompt surrender or proved destruction of any associated physical authenticators that store attribute certificates.

5.151 Attribute certificates, which are digital certificates, provide data that asserts particular attributes about the holder of the certificate—such as their identity attributes (for example, where a physical authenticator stores digital certificates that embed an individual's identity details such as name, date of birth, linkages to an Australian business, or other attributes, authorisation level, or roles). The certificates are signed digitally by the ISP, confirming their validity and integrity. A physical

authenticator that stores attribute certificates might come in various forms, such as smart cards, USB tokens, multi-factor cryptographic software or other hardware devices that can securely store and present these certificates as needed. The purpose of this rule is to ensure secure access to a digital ID by authenticating the bearer's credentials in a way that is difficult to forge or manipulate and to ensure that where an entity issues authenticators containing attribute certificates, that these authenticators are surrendered, revoked or destroyed where appropriate.

Rule 5.28 Revocation and termination of an authenticator

5.152 This rule prescribes requirements for the revocation and termination of an authenticator. Revocation of an attribute certificate and termination of an authenticator refers to removal of the binding between an authenticator and a digital ID the ISP manages.

5.153 Subrule 5.28(1) provides for the events which, if they occur, would require an ISP revoke an authenticator as soon as practicable.

5.154 Subrule 5.28(2) relevantly requires the ISP to ensure the individual cannot use the authenticator where the certificate is revoked, or the authenticator is terminated.

5.155 Subrule 5.28(3) provides a non-exhaustive list of the appropriate actions the ISP could take to ensure the revoked attribute certificate or terminated authenticator is not used, which depends on the authenticator type. For example, the ISP may ensure the surrender or proved destruction of any associated physical authenticators that store attribute certificates.

Division 4—Accessibility and useability

Rule 5.29 Application

5.156 This rule prescribes that this Division applies for the purposes of section 30 of the Digital ID Act, which relevantly provides that an accredited entity must take reasonable steps, including requirements to be set out in these Rules, to ensure that its accredited services are accessible for individuals who experience barriers when creating or using a digital ID.

Rule 5.30 Verification services

5.157 This rule prescribes the accessibility and useability requirements that an ISP must comply with in relation to the identity proofing process.

5.158 Subrule 5.30(1) relevantly requires an ISP to provide support to individuals who need assistance during the identity proofing process. This support must include providing clear instructions to an individual about how they can update their personal information held by the ISP. The intention of this requirement is to promote useability in the implementation of other rules that relate to reusable digital IDs, including rules 5.4, 5.5, and 5.6, which ensure a reusable digital ID continues to be maintained.

5.159 Additionally, this rule complements APP 10, APP 12 and APP 13 to ensure that an individual's personal information remains up-to-date, accurate and complete, and that an individual has access to update that information and correct it, should that be necessary. Other support might include, for example, an email address where an individual can contact the ISP for assistance with issues related to the identity proofing process, such as where a credential cannot be verified by an authoritative source, meaning the individual cannot complete the identity proofing process.

5.160 Subrule 5.30(2) relevantly requires an ISP to provide a clear and simple description of each step of the identity proofing process.

5.161 Subrule 5.30(3) requires an ISP to provide individuals with information about the technical requirements for using the ISP's accredited services. In practice, this could include information about access to a mobile phone or webcam.

5.162 Subrule 5.30(4) sets out the information and notification requirements that an ISP must provide to an individual when requesting to verify the individual's identity at a particular IP level. This includes providing information on the documents or other credentials that may be requested, which combinations of credentials are required to achieve a supported IP level and notifying individuals whether a requested document or other credential is mandatory. ISPs must also notify individuals undergoing the proofing process of the consequences if a credential is not provided for verification. For example, that the proofing process will suspend or terminate, and what will happen to the information that has already been provided up to that point in the process and when it would be deleted.

5.163 Subrule 5.30(5) broadly prescribes that ISP must inform the individual in advance using clear and simple terms, regarding the receipt and use of any digital codes that may be issued to an individual during the identity proofing process. Digital codes are commonly used at an early stage of identity proofing to prove the individual has

control of a nominated email account or mobile phone number. The intention of this requirement is to ensure that individuals have clear useability instructions in relation to receiving and verifying digital codes as part of the generation, management, maintenance or verification process for digital IDs. In some cases, the digital codes may be associated with an authenticator or be used as part of an authenticator issuance process. In those cases, certain obligations in relation to issuance of authenticators may apply to the entity under the Accreditation Data Standards.

5.164 Subrule 5.30(6) sets out the information that an ISP must communicate to individuals at the conclusion of the identity proofing process, depending on the outcome. To the extent that an individual has provided details of their identity and other credentials during an unsuccessful or partially completed identity proofing process, an ISP is broadly required to provide the individual with information about:

- how to complete the process,
- what will happen to the identity information that has been provided up to that point, and
- how to access alternative channels if the accredited entity supports alternative channels.

5.165 This rule is intended to support ISPs to provide consistent and accessible information about the identity proofing process.

5.166 Subrule 5.30(7) relevantly requires an ISP to notify the individual under subrule 5.30(6) as soon as practicable after the ISP knows the outcome of the identity proofing process.

5.167 Subrule 5.30(8) supplements subrule 5.30(6) by broadly providing that, to the extent practicable, an ISP must not require individuals who wish to continue an earlier proofing process to re-submit credentials that have already been verified; and that the ISP must as soon as practicable destroy information provided by individuals who do not wish to continue the proofing process at a later time and notify the individual that the information will be destroyed.

Rule 5.31 Authentication services

5.168 This rule sets out the requirements for an ISP that provides services involving the authentication of an individual.

5.169 Individuals must be informed as to how to use and maintain their authenticator, which could include its use to authenticate the individual during an online transaction with a relying party, as well as its use to access and manage details stored as part of the individual's digital ID. Individuals must also be informed of when the authenticator will expire, should the ISP provide authenticators that expire under rule 5.27.

5.170 This rule also requires individuals to be informed of what they should do if they believe their authenticator has been forgotten, lost or stolen. This could include directions on how to report this to the ISP and any steps that should be taken to ensure the individual's digital ID is not accessed or used by another person.

Part 5.2—Accredited attribute service providers

Rule 5.32 Verifying and managing a special attribute

5.171 This rule defines the term ***special attribute*** and sets out the requirements for verifying and managing a special attribute.

5.172 Subrule 5.32(1) provides that an ASP must only verify and manage an attribute of an individual if the particular kind of attribute is specified in the ASP's accreditation conditions as an attribute the ASP is accredited to verify and manage (i.e. a special attribute). Special attributes may include any attributes about an individual that can be verified or self-asserted and disclosed under the Digital ID Act.

5.173 For example, a special attribute may be an authorisation to act on behalf of a business, verified information relating to the qualifications of an individual such as a university qualification or trade qualification, or other information in relation to section 10 of the Digital ID Act. What the special attribute is and how it is described will be specified in the ASP's accreditation conditions. An ASP must also be aware of its obligations in relation to obtaining express consent from an individual prior to disclosing a special attribute, as required by rule 7.1. The process of verifying and managing a special attribute includes ensuring that the relevant attribute is the correct attribute in relation to the individual to whom the special attribute relates.

5.174 Subrule 5.32(2) relevantly provides that an ASP must determine the IP level it requires in respect of a special attribute it verifies and manages as part of its accredited services, and must not provide an accredited service in respect of an individual unless the digital ID of the individual meets that IP level.

5.175 This subrule recognises that some special attributes may be considered more sensitive than others. For example, a special attribute that identifies the individual as a holder of a recreational fishing licence may be less sensitive than a special attribute that identifies the individual as a holder of a registered licence to practice medicine or registered member of another profession. The intention of this rule is to ensure that ASPs manage the access and process to verify a special attribute, including potential risks and impacts to individuals and relying parties should a special attribute be verified or disclosed to the incorrect individual, either by means of fraud being committed or by mistake (e.g. if the attribute is not matched with the correct individual).

Rule 5.33 Requirements when verifying a special attribute

5.176 This rule sets out the requirements for an ASP when verifying a special attribute.

5.177 An accredited entity that is an ASP may also be the authoritative source for the attribute(s) for which it is accredited as an ASP to verify and manage. However, the accreditation of an ASP is not intended to extend to the processes at the authoritative source for the issuance of documents or other credentials containing information about an individual. The process for verifying an individual's special attribute is determined by the requirements of the authoritative source that issues that special attribute.

5.178 Subparagraph 5.33(a)(i) provides that when verifying a special attribute of an individual, the ASP must ensure that the special attribute verified is unique to the

individual. This ensures that each special attribute can only be related back to one individual (for example University Degree XYZ1234 is unique to Jasmine Wu) and cannot be "claimed" as a verified special attribute by 2 or more individuals.

5.179 The intention of this requirement is to provide relying parties who require a special attribute with confidence in the verification and disclosure processes for that special attribute. Additionally, it assists in mitigating digital ID fraud risks and incidents where a malicious actor might attempt to fraudulently claim a special attribute to gain access to a relying party's services. For example, a malicious actor claiming a special attribute that authorises them to act on behalf of a business may then be able to submit false information for monetary gain.

5.180 Subparagraph 5.33(a)(ii) requires that the ASP must ensure that a special attribute is current at the time it is verified. Practically, this ensures that an ASP cannot consider a special attribute as verified where that special attribute has no determined processes at the authoritative source for determining if the special attribute has expired or can be revoked in the case of a fraud or security incident. An example of a process to determine that a special attribute verified with an authoritative source is current would be where individual Mathew Chiu is trying to verify that special attribute medical licence ABC5678 belongs to them. However, medical licence ABC5678 has been cancelled due to an incident of malpractice and that special attribute is therefore not current.

5.181 Paragraph 5.33(b) sets out the requirements for the process of verification of a special attribute with the authoritative source including that the connection must be secure, trusted and facilitated using approved cryptography. This ensures that any personal information is protected where that information is disclosed to the authoritative source to verify a special attribute. Additionally, the ASP must comply with requirements set by the authoritative source to confirm that the special attribute is unique to the individual so that the special attribute can be verified.

Rule 5.34 Special attributes that are self-asserted

5.182 This rule sets out the requirements for an ASP in relation to special attributes that are self-asserted by the individual.

5.183 An ASP may allow an individual to provide information and attributes about themselves to support the verification of their digital ID at a relying party service. A special attribute that is self-asserted is one that has not been verified by an authoritative source in accordance with rule 5.33. This rule is intended to support attributes that may not be (or cannot be) verified with an authoritative source but are still associated with the individual's digital ID. This could include an individual's postal address which may be useful to be provided as a self-asserted attribute so that the individual does not need to re-type the same information for multiple services where this is required. This rule seeks to ensure that where an ASP provides a special attribute that is self-asserted, the ASP must inform another accredited entity or relying party of that fact. That way, the provenance of information is known for different types of attributes, and that self-asserted attributes are not treated with the same trust and reliance as special attributes that are verified in accordance with Part 5.2 of the Rules.

Rule 5.35 Special attributes affected by a fraud or cyber security incident

5.184 This rule sets out the requirements for an ASP in circumstances where a special attribute has been affected by a digital ID fraud or cyber security incident.

5.185 Subrule 5.35(1) is broadly requires an ASP to have processes in place to ensure that a special attribute involved in a cyber security or digital ID fraud incident is not disclosed to relying parties or other entities who may wish to rely on it. This prevents a special attribute that may be compromised (as far as the ASP is aware) from being provided to other parties to rely on.

5.186 Subrule 5.35(2) requires that if an ASP is aware that a special attribute has been involved in a cyber security incident or digital ID fraud incident, it must immediately notify the authoritative source (if the ASP and authoritative source are not the same entity). An example of a digital ID fraud incident may include where the digital ID of an individual with the special attribute that has been disclosed is subject to a digital ID fraud incident that has been reported across a digital ID system. An example of a cyber security incident may include where a relying party has been subject to a data breach and the special attribute that was disclosed to that relying party has been compromised. This rule helps to ensure that where an authoritative source is a third party and not subject to the accreditation scheme, or is operating in a different digital ID system, the authoritative source is aware that the special attribute may be compromised and can take steps to make any other services outside digital ID system that rely on that attribute aware of existing cyber security or fraud risks.

Part 5.3—Accredited identity exchange providers

5.187 This Part sets out rules specific to an accredited IXP. The role of an IXP is to orchestrate the flow of information between participants in a digital ID system by securely authenticating and identifying the participants in a transaction. As with other types of services accredited under the Digital ID Act, it is expected that the conditions of accreditation will generally cover the types of services an accredited IXP will operate. This includes determining the architectural model and operational context of the IXP. Unlike ISPs or ASPs, an IXP generally cannot operate without other digital ID services on a digital ID system. This is because its purpose is to assist those other accredited services such as ISPs or ASPs or third-party entities (unaccredited entities) to connect to relying parties and convey, manage and coordinate the flow of information from those services to relying parties.

5.188 There are different types of exchange models, which mean the Rules will apply in different ways depending on the architecture of the IXP. This includes the configuration of the IXP's DI data environment, its operational context, which digital ID system(s) it operates within, and the digital ID system(s) governance arrangements. These things also impact other kinds of accredited services, but an IXP is unique in its role in that it has the technical capacity to determine or apply governance arrangements for other participants in its digital ID system, and provides a central assurance role in the effective ongoing governance of that digital ID system. Technical capacity in relation to this may be, for example, the ability to cut off an entity's access to the digital ID system.

5.189 The TDIF pilot accreditation program that operated prior to the commencement of the Digital ID Act accredited 2 kinds of architectural models of IXPs. Broadly, these involve:

- a technical integration point for participants in what is often called a 'brokered' or 'hub and spoke' model for a digital ID system. The IXP sits in the middle of all participants, mediating all interactions and the conveyance, management and coordination of information between participants, or
- a technical 'register' that coordinates interactions between participants in its digital ID system by verifying the participants and facilitating the flow of information between those participants. In this model, the IXP may not directly convey the data or information between those participants as in the brokered or hub and spoke model.

Rule 5.36 General Requirements

5.190 This rule sets out the general requirements for an IXP.

5.191 This rule is intended to ensure that an IXP has the technical capacity to securely convey, manage and/or facilitate the flow of data or other information to participants in the digital ID system in which the IXP operates. This rule provides assurance that an IXP can securely identify and authenticate participants in its digital ID system prior to data and other information, which may be personal information, being disclosed from ISPs, ASPs or other entities to relying parties. This promotes trust between participants in a digital ID system (i.e. entities can rely on the information that is conveyed, managed or coordinated between them) and amongst individuals who access relying party and digital ID services via an accredited exchange.

Rule 5.37 Digital ID system rules

5.192 This rule prescribes the requirements for the governance arrangements that must apply to a digital ID system, other than the AGDIS, in which IXP operates and provides its services.

5.193 The requirements in these rules do not apply to an IXP onboarded to the AGDIS as the AGDIS is regulated by the Digital ID Act and the Digital ID Rules, which set out governance provisions that apply to all entities participating in the AGDIS. The intention of rule 5.37 is to promote the integrity of the accreditation scheme as it applies to an IXP operating and providing its services in a digital ID system where not all other service providers are accredited. This is achieved by requiring that an IXP that operates in such a digital ID system can technically facilitate governance arrangements via system rules to extend some core privacy protections and security controls to those unaccredited service providers.

5.194 Subrule 5.37(1) relevantly prescribes that this rule applies to an IXP operating in a digital ID system other than the AGDIS and where one or more entities participating in the digital ID system provides digital ID services in the system that are not accredited services. For example, this could include entities from the financial services sector that provide similar identity checks under KYC activities or ISPs providing digital ID services to relying parties via the IXP that are not subject to the privacy and security protections in the Digital ID Act.

5.195 Subrule 5.37(2) relevantly provides that an IXP must ensure that the digital ID system that it operates in is subject to system rules which meet the requirements set out in this subrule. System rules, also known as 'trust frameworks', in respect of digital ID systems, are governance arrangements and requirements that enable entities participating in a digital ID system to trust each other by ensuring that they are all subject to the same requirements and arrangements. System rules also define the scope and purpose of the digital ID system. The system rules often determine what operational roles are to be included and what duties are assigned to those roles (such as ISP, relying party etc.). They often set the eligibility requirements for entities seeking to fulfil those roles and establishes rules and for how information is to be processed within the relevant digital ID system.

5.196 Paragraph 5.37(2)(a) sets out the requirements for the system rules in terms of who they must apply to and how the system rules must be enforced. In this case the system rules must be binding on an ISP that provides services within the system that are not accredited services (referred to in this rule as an unaccredited ISP).

5.197 Paragraph 5.37(2)(b) requires that the IXP, or another person, must be able to revoke an unaccredited ISP's participation in the digital ID system for non-compliance with the system rules. This is an important security measure that promotes assurance in an IXP's accredited services in that it can technically enforce system rules to the extent that if an unaccredited ISP were to breach the system rules, an IXP could revoke the use of the unaccredited ISP's services in the digital ID system by refusing to convey, manage and coordinate the flow of information for that unaccredited ISP.

5.198 Paragraph 5.37(2)(c) requires that the system rules are not inconsistent with the Digital ID Act and the Rules. This means that the system rules cannot, for example, explicitly permit or require a type of control or action that is prohibited in the Digital ID Act. This does not mean that the system rules must be *consistent* with the Digital

ID Act and the Rules, which may require relevant provisions of the Digital ID Act and the Rules to be incorporated into system rules. The system rules could include matters that are not addressed by the Digital ID Act or the Rules. The policy objective is to ensure that an IXP operating in a digital ID system with unaccredited ISPs cannot have system rules that explicitly allow conduct by unaccredited ISPs that would not be permitted under the Digital ID Act or the Rules.

5.199 This provision is further supported by the subsequent paragraphs in this rule, which provide that unaccredited ISPs must be subject to additional requirements and those requirements must be included in the system rules. These requirements are privacy protections and security controls that protect individuals' personal information within a digital ID system in which an IXP operates.

5.200 Paragraph 5.37(2)(d) broadly has the effect that unaccredited ISPs are subject to the requirements to protect personal information in transit and at rest in accordance with approved cryptography outlined in rule 4.21. This is particularly important to ensure that where the system is coordinating the disclosure of an individual's personal information directly from an unaccredited ISP to a relying party, for example by a 'register' type of exchange, that that personal information is encrypted in transit in accordance with the high standards set out in the ISM.

5.201 Paragraph 5.37(2)(e) requires that an unaccredited ISP must not disclose an attribute of an individual referred to in section 45 of the Digital ID Act without obtaining the express consent of the individual. This is a core privacy protection of the Digital ID Act and is a mandatory privacy protection that extends to unaccredited ISPs for which the accredited IXP may convey, manage and coordinate the flow of information.

5.202 Paragraph 5.37(2)(f) prohibits one-to-many matching of biometric information of an individual collected for the purposes of the ISP doing either or both verifying the identity of the individual or authenticating the individual to their digital ID. This reflects a prohibition in the Digital ID Act on accredited entities conducting one-to-many matching in their accredited services. ***One-to-many matching*** is defined in subsection 48(4) of the Digital ID Act.

Chapter 6—Annual reviews

6.1 Accredited entities are required to conduct annual reviews to maintain their accreditation. The purpose of an annual review is to ensure that the Digital ID Regulator remains satisfied that the accredited entity continues to meet accreditation requirements over time. It also helps ensure that an accredited entity continues to manage risks appropriately as both technology and the risk landscape changes. Generally, an entity would be required to submit an annual report from the accredited entity's accountable executive, which attaches copies of required assurance assessments and systems testing reports as well as copies of other documents as necessary, to demonstrate that required controls have been effectively maintained.

Part 6.1—Accredited entities to conduct annual reviews

Rule 6.1 General requirements

6.2 Subrules 6.1(1) and (2) prescribe the general requirements for an accredited entity to conduct an annual review and give a copy of that report to the Digital ID Regulator.

6.3 Subrule 6.1(3) provides that the assurance assessments, systems testing, and other testing conducted for an annual review must be conducted as close as practical to the end of the reporting period for that annual review. The purpose of this subrule is to minimise the risk that the reports provided to the Digital ID Regulator are out of date or impacted by other changes made to the entity's DI data environment after the assurance assessment, system testing or other testing has been completed.

Rule 6.2 Reporting periods

6.4 This rule prescribes the reporting periods for transitioned accredited entities and other accredited entities. Generally, a reporting period falls on the same date each year. For an accredited entity which is not a transitioned accredited entity, that reporting period is to be 12 months starting on the day the entity's accreditation comes into force as per subrule 6.2(4).

6.5 Due to the transitional arrangements for entities accredited under the TDIF pilot accreditation program, it was appropriate to allow transitioned accredited entities to nominate their annual review date. However, a transitioned accredited entity wishing to select an annual review date must nominate a date in accordance with subrule 6.2(1). This is to allow a transitioned accredited entity to select a date that better suits their business needs rather than the date on which the Digital ID Act commences, which is the default annual review date under subrule 6.2(3) if the entity does not nominate a different date.

Rule 6.3 Scope of annual review

6.6 This rule sets out the scope of an annual review for an accredited entity.

6.7 Subrule 6.3(1) broadly requires accredited entities to, for each reporting period, identify any changes to its DI data environment and accredited services that may affect its ability to comply with the Digital ID Act, the Rules and the Accreditation Data Standards.

6.8 Subrule 6.3(2) broadly requires an accredited entity to consider the impact of each change on its accredited services, DI data environment, and ability to comply with the Digital ID Act, the Rules or the Accreditation Data Standards to assess if the change is material. When considering the impact of an individual change, accredited entities must not only consider the change in isolation, but also alongside other changes that have been made since the last annual review was conducted. This is because iterative changes in an entity's DI data environment are expected and a normal part of IT system operation, and small iterative changes may, cumulatively, constitute a material impact to the entity's accredited services or DI data environment.

6.9 The policy intention for this rule is to ensure that an accredited entity tracks material changes that may include, but are not limited to, changes that materially or adversely affect an entity's ability to comply with the Digital ID Act, the Rules or the Accreditation Data Standards. This is required to provide the Digital ID Regulator with assurance that the entity's DI data environment and accredited services continue to comply with the Digital ID Act and the Rules on an ongoing basis.

6.10 The purpose of subrule 6.3(2) is for an accredited entity to keep track of material changes that might require updated assurance assessment or system testing reports to be submitted to the Digital ID Regulator to demonstrate their compliance with the relevant provision where a material change occurs.

6.11 For paragraph 6.3(2)(c), the policy intention is for the accredited entity to include in its statement of scope and applicability information on the reasons for certain controls and requirements being affected by the material change when the statement is provided to the assessor conducting the assurance assessment or system testing.

6.12 **Example 1:** An entity makes a series of small changes to its processes for managing digital ID fraud incidents. Each of those changes are not considered material alone but over time, when considered cumulatively in the context of the assessed compliance with the investigation of digital ID fraud incidents, these changes may be considered a material change.

6.13 **Example 2:** An accredited entity procures a new fraud detection system that it integrates into its DI data environment and accredited services. The new fraud detection system may be better than the old fraud detection system, meaning that this change could be viewed as a positive advancement of the entity's digital ID fraud management capability. However, the accredited entity's compliance with the fraud detection and investigation rules (rules 4.33 and 4.34) have not been assessed as compliant with the new operational fraud detection system. In these circumstances, the system change could be considered a material change as it may affect the entity's obligations to comply with those relevant rules that the change affects.

6.14 Subrule 6.3(3) broadly requires accredited entities to conduct a range of assurance assessments, system testing, technical testing, testing of PAD technology and various other biometric-related testing in relation to the material change identified. The assessment or testing is generally only appliable to the extent relevant to the material change. The purpose of the assessment or testing is to determine that the material change has been assessed or tested as being able to continue to meet the controls and requirements under the Digital ID Act, the Rules or the Accreditation Data Standards that are affected by the material change.

6.15 For example, migrating accredited services from one cloud service provider platform

to another could involve material changes to the underlying technical environment. Therefore, the efficacy of cyber security controls must be re-verified through a protective security assessment, while other elements of the Rules such as accessibility, usability and inclusion requirements for public-facing services may not be impacted at all by such a change.

6.16 Subrule 6.3(4) requires accredited entities to review any condition imposed by the Digital ID Regulator relating to the collection and disclosure of restricted attributes by the entity to determine if the condition continues to be required. This is an important privacy protection that acknowledges the changes to the broader identity landscape, including whether relying parties may no longer necessarily need to collect restricted attributes, such as where regulation or regulatory guidance applicable to the relying parties' identity verification obligations is updated. This rule complements paragraph 6.9(e), which together requires an accredited entity to provide confirmation that conditions related to restricted attributes continue to be necessary and appropriate in its attestation statement.

Rule 6.4 Assurance assessments

6.17 This rule sets out the required frequency of fraud assessments and protective security assessments and provides exceptions to the fraud assessment assessor requirements set out in subrule 3.6(2).

6.18 In general, fraud and protective security assessments must be conducted by an independent assessor every 2 years. This is because fraud and protective security are domains where the digital ID fraud and cyber security risk landscape and attackers are constantly evolving, and it is important to regularly assess whether the accredited entity's implemented controls and compliance with the Rules remains effective.

6.19 Subrule 6.4(2) generally provides an exception to the requirements set out in subrule 3.6(2) regarding the assessor's association with and independence from the accredited entity.

6.20 The intention of this subrule is to enable an accredited entity who has demonstrated that its fraud management capability is sufficiently mature to enable its personnel who meet the assessor requirements as per rule 3.2 to conduct the fraud assurance assessment. This is because some accredited entities have large scale fraud capabilities due to the kinds of services (both accredited and unaccredited) they provide, and in some cases, it may be appropriate to allow these personnel to conduct fraud assurance assessment every second year.

6.21 However, subrule 6.4(2)(a) broadly requires that if an accredited entity relies on this provision, it must ensure its next fraud assurance assessment is conducted by an independent assessor pursuant to rule 3.2 (this effectively allows the independent assessment requirements to be required once every 4 years, not taking into consideration any assessments that are prompted by material changes).

Rule 6.5 Penetration and presentation attack detection testing

6.22 This rule prescribes the testing frequency for penetration testing and PAD testing. The effect of this rule is that an accredited entity must conduct penetration testing for each reporting period and provide its response to the assessor's report. An ISP that conducts biometric binding or biometric authentication is required to conduct

testing for PAD in its second reporting period and every alternate reporting period thereafter.

6.23 The frequency for penetration testing is set at yearly to help ensure that an accredited entity effectively manages cyber security risks to its accredited services and has implemented effective protective security controls to detect and prevent malicious attackers from gaining access to its IT systems. This is particularly important in the realm of cyber security risks due to the rapid increase and dissemination of new technology and techniques that exploit vulnerabilities in IT systems.

6.24 Similarly, PAD testing is required every second year to help ensure that an accredited entity's PAD technology continues to mitigate common attacks. Similar to penetration testing, this is because the types of attacks that may have been difficult for an average individual to perpetrate without access to significant resources become easier due to the rapid increase and dissemination of new technology. An example of this is the advent and rapid development and availability of 3D printing, making it easier to create latex masks or other items to assist an individual in fooling PAD technology.

Part 6.2—Accredited entities to provide annual reports

6.25 This Part contains rules that relate to the content of, and attachments to, the accredited entity's annual review report that is submitted to the Digital ID Regulator.

Rule 6.6 Content of annual report

6.26 This rule prescribes the general requirements for the content of the annual report.

Rule 6.7 If previous timeframes to address risks and recommendations not met

6.27 This rule broadly requires an accredited entity to include in its annual report the details of any measures that the entity has failed or is likely to fail to implement in accordance with the recommended timeframe. This applies to a PIA under rule 2.4 or an assessor's report under rule 3.17 and the entity's response to that report as per rule 3.18.

6.28 The purpose of this rule is to ensure that the accredited entity remains accountable for implementing risk treatments or recommendations in the entity's response to an assessor's report or the PIA and agreed by the entity's accountable executive. This includes ensuring that the accredited entity provides an updated timeframe and details of the risks that arise or are likely to arise from the treatment not having already been implemented. The intention of this rule is to promote accredited entities to maintain an appropriate risk management capability in relation to the treatment or recommendation, particularly where the risk may increase as a result of the treatment or recommendation having not been implemented.

Rule 6.8 Information and documents

6.29 This rule prescribes the information and documents that must be included in the accredited entity's annual report. As per rule 6.1, the report must be submitted to the Digital ID Regulator.

Rule 6.9 Attestation statement

6.30 This rule prescribes that the annual report must include an attestation statement and sets out the requirements for that statement. The purpose of this rule is to ensure that the accredited entity's accountable executive has oversight of the entity's ongoing compliance with the Rules and can attest to its ongoing compliance and risk management. It also seeks to ensure that the executive is accountable for the information provided to the Digital ID Regulator.

Chapter 7—Other matters relating to accreditation

Part 7.1—Matters related to attributes

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

7.1 This rule prescribes additional attributes for which accredited entities must obtain express consent before disclosing to relying parties. These are in addition to the attributes set out in section 45 of the Digital ID Act. This rule is made for the purposes of paragraph 45(f) of the Digital ID Act.

Rule 7.2 Meaning of *restricted attribute* of an individual

7.2 This rule prescribes an attribute which is a restricted attribute, in addition to those prescribed by section 11 of the Digital ID Act. These attributes are a number on a document or other credential listed in Schedules 1 to 4 that is a unique identifier for that particular version of the document or other credential. This rule is made for the purposes of paragraph 11(1)(f) of the Digital ID Act.

7.3 For example, a unique identifier for a driver's licence is the card number of that version of the licence. An Example of a unique identifier for a driver's licence is provided in this rule.

Part 7.2—Accreditation conditions

Rule 7.3 Table of accreditation conditions

7.4 Section 17 of the Digital ID Act broadly provides that the accreditation of an entity may be subject to conditions imposed by the Digital ID Regulator or by the Rules.

7.5 This rule sets out the accreditation conditions and associated circumstances of those conditions for various kinds of accredited entities for the purposes of subsection 17(5) of the Digital ID Act. These conditions are in addition to those prescribed by or under subsections 17(1) and (2) of the Digital ID Act.

7.6 The conditions prescribed by this rule address common kinds of conditions that will be required to be placed on an accredited entity by virtue of the kind of accredited service it provides and, where applicable, the rules it must comply with. For example, the condition on accreditation in item 6 of the table in this rule will need to be placed on an ISP that is providing an accredited service to IP3 by completing online biometric binding utilising source biometric matching. This is due to the need for a condition to authorise the collection of an image provided by the individual (biometric information) in order to complete online biometric binding for IP3.

Part 7.3—Reportable incidents

Rule 7.4 Reportable incidents

7.7 This rule prescribes the activities and circumstances that an accredited entity must notify the Digital ID Regulator of within 5 business days. The purpose of these requirements is to ensure that the Digital ID Regulator is aware of any material changes to an accredited entity's circumstances and DI data environment that may affect its compliance with the Digital ID Act and the Digital ID Regulator's decision to accredit the entity.

Rule 7.5 Change of control for corporations

7.8 This rule applies the definitions of terms that are used in the *Corporations Act 2001* and prescribes the notification requirements for when there is a change in control, or a proposed change in control, of an accredited entity that is a corporation, or an entity that is a corporation whose accreditation is suspended.

7.9 Subrule 7.5(6) prescribes the timeframes for when the notification must be made to the Digital ID Regulator. Paragraph 7.5(6)(a) provides for a timeframe of within 72 hours after the entity becomes aware that a change in control will occur. Paragraph 7.5(6)(b) provides for a timeframe of within 72 hours after the change in control occurs, such as in circumstances of a hostile takeover, where the entity and its personnel are not aware of a change in control until it happens.

7.10 Subrule 7.5(7) provides for the circumstances in which an entity is taken to be aware of a change in control. Generally, this is at the time the entity has passed a resolution regarding the change in control, or when a court order regarding the change in control is made.

Rule 7.6 Entity no longer providing accredited services

7.11 This rule prescribes that if an accredited entity intends to cease providing accredited services, it is required to inform the Digital ID Regulator of its intention and details of its plans as soon as practicable after forming that intent. The purpose of this rule is to ensure the Digital ID Regulator has all relevant information which may assist and inform its ability to perform its functions.

Part 7.4—Data standards relating to accreditation

Rule 7.7 Digital ID Data Standards Chair to make standards

7.12 This rule relevantly provides that the Data Standards Chair must make one or more of technical, data or design standards relating to accreditation, for the matters specified in subrule 7.7(2). This rule is made for the purposes of paragraph 99(1)(c) of the Digital ID Act, and additional matters on which the Data Standards Chair may make standards are set out in section 99 of the Digital ID Act.

7.13 The Accreditation Data Standards to be made pursuant to this rule are of a technical nature, prescriptive and may need to be updated more frequently than the Rules to, for example, to quickly address the rapidly changing risk and technology landscape. The Accreditation Data Standards made in relation to the matters in subrule 7.7(2) relate broadly to authentication management and the testing of biometric technology used in biometric binding solutions, including the testing of a biometric matching algorithm, PAD technology and eIDVT solutions.

Part 7.5—Record keeping

Rule 7.8 General record keeping requirement

7.14 This rule prescribes the circumstances in which an accredited entity must not destroy or de-identify certain personal information it possesses or controls; and which the accredited entity is required or authorised to retain by or under the Digital ID Act (including the Rules or the Digital ID Rules), a direction issued by the Digital ID Regulator under section 127 of the Digital ID Act, or a court/tribunal order within the meaning of the Privacy Act.

7.15 The information that must not be destroyed nor de-identified under this rule is required to be retained to assist the Digital ID Regulator to perform its functions. This is intended to prevent accredited entities that become aware that they are under scrutiny by the Digital ID Regulator, or undergoing other legal proceedings, from destroying relevant records. These records may be required for the Digital ID regulator's investigations, or to support other legal proceedings.

7.16 Rule 7.8 is intended to cover situations where, for example, due to actions by the Digital ID Regulator, the accredited entity holds information which is related to anticipated legal proceedings. In that situation, the accredited entity would be prohibited from destroying records related to the anticipated legal proceedings under this provision.

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

7.17 Schedule 1 contains a table of documents or other credentials that are ***CoI credentials***, defined in rule 1.4. A CoI credential evidences an individual's commencement of identity in Australia. Column 2 indicates the available methods that an ISP should use to verify the credential to confirm the details presented are accurate and current.

7.18 Column 2 does not necessarily mean that the documents or credentials listed are publicly available to be verified via this method (in the case of source verification).

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

7.19 Schedule 2 contains a table of documents or other credentials that are ***linking credentials***, as defined in rule 1.4. A linking credential demonstrates the continuity of the individual's verified identity where that individual's attributes have changed, such as item 2, being a change of name certificate. Column 2 indicates the available methods that an ISP should use to verify the credential to confirm the details presented are accurate and current.

7.20 Column 2 does not necessarily mean that the documents or credentials listed are publicly available to be verified via this method (in the case of source verification).

Schedule 3—Documents or other credentials that are a UitC credential

7.21 Schedule 3 contains a table of documents or other credentials that are ***UitC credentials***, as defined in rule 1.4. A UitC credential evidences an individual's use in the Australian community of that individual's identity. Column 2 in the table indicates the available methods that an ISP should use to verify the credential to confirm the details presented are accurate and current.

7.22 Column 2 does not necessarily mean that the documents or credentials listed are publicly available to be verified via this method (in the case of source verification).

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

7.23 Schedule 4 contains a table of documents or other credentials that are ***photo IDs***, defined in rule 1.4. A photo ID is a document or other credential that includes an image of an individual (biometric information), which can be used for biometric binding at higher IP levels. Photo IDs may also be used as a UitC credential as per item 7 in Schedule 3. Column 2 indicates the available methods that an ISP should use to verify the credential to confirm the details presented are accurate and current.

7.24 Column 2 does not necessarily mean that the documents or credentials listed are publicly available to be verified via this method (in the case of source verification).

Schedule 5—PSPF controls

7.25 Schedule 5 lists applicable protective security requirements and requirements within

the PSPF that must be implemented by accredited entities who elect to implement the PSPF as their selected protective security controls framework under rule 4.3.

ATTACHMENT B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Digital ID (Accreditation) Rules 2024

The *Digital ID (Accreditation) Rules 2024* (the Rules) are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Rules

The Rules establish a robust and effective legal framework governing the accreditation scheme, and the obligations of accredited entities as approved to operate an accredited digital ID service. In particular, the Rules include details on:

- requirements for applying for accreditation;
- assurance assessments and systems testing, including penetration testing, usability testing, security and fraud assessments;
- requirements for maintaining accreditation, including certain protective security, fraud, privacy controls, useability testing, accessibility and inclusion requirements;
- requirements and controls for each kind of accredited service, Identity Service Provider (ISP), Attribute Service Provider (ASP) and Identity Exchange (IXP);
- requirements on the annual review of accreditation, including whether the entity continues to comply with the applicable law; and
- other matters relating to accreditation, such as the accreditation conditions on an entity.

Human rights implications

The Rules positively engage the following rights:

- the right to protection from arbitrary or unlawful interference with privacy contained in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR), and also referred to in Article 16 of the *Convention on the Rights of the Child* (CROC) and Article 22 of the *Convention on the Rights of Persons with Disabilities* (CRPD).
- the rights of parents and children, contained in Article 3 and 12 of the CROC and Article 24(1) of the ICCPR.
- the rights of persons with disability to live independently and participate fully in all aspects of life and to access, on an equal basis, community services and facilities and

to access information in accessible formats and technologies, consistent with Articles 9(1), 19(c) and 21 of the CRPD.

- the rights to equality and non-discrimination, contained in Article 26 of the ICCPR and Article 2 of the CROC.

PROTECTION FROM ARBITRARY OR UNLAWFUL INTERFERENCE WITH PRIVACY

Article 17 of the ICCPR prohibits arbitrary or unlawful interference with privacy. It states that:

- *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
- *Everyone has the right to the protection of the law against such interference or attacks*.

Article 16 of the CROC and Article 22 of the CRPD contain similar rights.

MEASURES TO PROTECT FROM ARBITRARY OR UNLAWFUL INTERFERENCE WITH PRIVACY

The Rules improve the right to protection from arbitrary or unlawful interference with privacy because they complement the privacy safeguards in the Digital ID Act by further limiting the collection, use and disclosure of personal information.

The Digital ID Act requires that accredited entities continue to comply with existing privacy protections in the Privacy Act or, for State or Territory entities, the relevant local privacy law. Where a State or Territory entity is not subject to a local privacy law, and wishes to become an accredited service provider, the Digital ID Act prescribes that the entity must enter into a binding agreement that would require them to comply with the Australian Privacy Principles (APPs. Australian Government agencies that are subject to the Privacy Act are also subject to the privacy governance code. In the context of the Rules, if an accredited entity is not an agency within the meaning of the Privacy Act, it must still comply with the privacy governance code in respect of its DI data environment and accredited services as if it were an agency for the purposes of the code.

The strict requirements for entities to become accredited and maintain their accreditation are intended to encourage the responsible handling of personal information to protect privacy. For example, Part 4.3 of Chapter 4 of the Rules requires accredited entities to comply with the privacy governance code, and they must have a privacy policy and a privacy management plan in place. An accredited entity must review these documents annually as per the annual review requirements in Chapter 6 of the Rules. The accreditation process has been designed to provide assurance to individuals that accredited entities are managing personal information properly and securely.

In addition to these requirements, Part 7.2 of Chapter 7 of the Rules impose conditions on accreditation of an accredited entity or class of entity. For example, the conditions only permit the collection, use or disclosure of an individual's attributes or restricted attributes by an accredited entity in limited circumstances. These conditions on accreditation are intended

to provide strengthened protection to enhance the enjoyment of the right to privacy and informational privacy.

The data minimisation principle in Rule 4.42 complements the accreditation conditions to enhance privacy outcomes of individuals. It limits the collection and disclosure of personal information from an accredited entity's accredited services to reduce the unnecessary sharing of personal information for the purpose of verifying an individual's identity. Accredited entities must also have the technical capability for relying parties to request and receive only the necessary personal information needed to provide its services.

Additionally, any personal information collected by an accredited entity to provide its accredited services must be managed in accordance with the privacy requirements and safeguards in the Digital ID Act. These measures are considered privacy enhancing because they help ensure that only the necessary minimum amount of personal information is collected to provide accredited services and disclosed to relying parties.

As required by the Digital ID Act, accredited entities must also obtain the express consent of an individual to collect, use and disclose the individual's personal information. The duration of the express consent is limited by the Rules to a maximum of 12 months. This corresponds with the good privacy practices outlined in the APP Guidelines. Hence, the Rules give individuals the choice to continue to give or vary or withdraw their express consent for accredited entities to securely collect, use and disclose their personal information.

Finally, accredited entities are required by the Rules to provide advice to individuals on how to safeguard their digital ID against fraud, and by extension, how to better protect their personal information. This gives individuals the knowledge to make informed choices about their privacy and self-protect against unlawful or arbitrary interferences to their privacy.

MEASURES TO ENSURE LIMITATIONS ON A PERSON'S PRIVACY ARE NOT ARBITRARY NOR UNLAWFUL

There are limited circumstances when personal information may be used and disclosed without the express consent of the individual. Personal information may generally be used and disclosed by accredited entities to prevent, detect, manage and investigate digital ID fraud incidents. This exception to the requirement for express consent is in place because accredited entities must prevent, detect and investigate digital ID fraud incidents under rule 4.34.

However, individuals must be notified that their personal information may be use and disclosed for digital ID fraud activities under rule 4.43. This gives individuals greater transparency on the operation of accredited services, how their personal information may be used, and visibility of emerging fraud or privacy issues. Individuals may also choose to suspend or deactivate their digital ID if they have concerns. To ensure this limitation is reasonable and not arbitrary or unlawful, the Rules put in place mechanisms for preventing, detecting, investigating and responding to these types of incidents and protective measures relating to the use and disclosure of personal information for these purposes.

For these reasons, this limitation to the right to privacy is reasonable, necessary and proportionate.

CONCLUSION

Despite engaging Article 17 of the ICCPR, the Rules promote the growth of, and trust in, digital ID services throughout the economy. The Rules ensure that individuals are informed about instances where their privacy may have been interfered with and are able to make decisions to protect their personal information. The limitations on privacy are permissible as they are reasonable, necessary and proportionate to give effect the objectives of the Digital ID Act.

THE RIGHTS OF PARENTS AND CHILDREN

Article 24(1) of the ICCPR states that:

> *Every child shall have, without any discrimination as to race, colour, sex, language, religion, national or social origin, property or birth, the right to such measures of protection as are required by their status as a minor, on the part of their family, society and the State.*

Article 3(1) of the CROC states that:

> *In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.*

Article 12(1) of the CROC states that:

> *States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.*

MEASURES TO PROTECT CHILDREN AND ENHANCE THEIR PRIVACY

Rule 5.2 operates to protect the rights and enhance the privacy of children because it specifies that children under 15 years of age cannot request to generate a digital ID. This is intended to enhance children's privacy as they may not have the capacity to understand, give informed consent and make decisions about their personal information or getting a digital ID.

The minimum age requirement is consistent with the APP Guidelines, in which individuals under the age of 15 are presumed not to have the capacity to consent. There is no universally agreed age where a young person is understood to have gained the capacity to consent, however, the age range of 13 to 16 years appears to be the most used and is supported by the principle of an evolving capacity in children as reflected in the CROC. Children under the age of 15 can still access government services using alternative ways.

The Transitional Act made consequential amendments to Schedule 2 of the ADA that will commence at the same time as the Digital ID Act commences. These amendments will permit the prescription of a minimum age for generating a digital ID in the Rules. This policy strikes a balance between providing children with the autonomy to give informed consent and providing safeguards and protections for children's privacy.

For these reasons, the limitations on the rights of parents and children are permissible as they are reasonable, necessary and proportionate to give effect to the objectives of the Digital ID Act.

For transitioned accredited entities, the application of rule 5.2 is delayed for 12 months from the commencement date of the Digital ID Act. This means that this rule is not applicable for the first 12 months post-commencement for accredited entities who are transitioning from the TDIF pilot accreditation program to the legislated accreditation scheme. Delaying the application of this rule by 12 months will engage this human right, but the engagement is reasonable, necessary and proportionate given the limited current use cases for children under the age of 15 creating and using digital IDs. In addition, rule 5.2 is a new rule which was not in the TDIF pilot accreditation program. Compliance with this rule requires transitioned accredited entities to implement IT system changes and therefore, it is reasonable and appropriate to give these accredited entities time to comply.

THE RIGHTS OF PERSONS WITH DISABILITIES TO PARTICIPATE FULLY

Article 9 provides for the right to accessibility. Article 9(1) of the CRPD states:

> *To enable persons with disabilities to live independently and participate fully in all aspects of life, States Parties shall take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, to the physical environment, to transportation, to information and communications, including information and communications technologies and systems, and to other facilities and services open or provided to the public, both in urban and in rural areas. These measures, which shall include the identification and elimination of obstacles and barriers to accessibility, shall apply to, inter alia:*
>
> a. *Buildings, roads, transportation and other indoor and outdoor facilities, including schools, housing, medical facilities and workplaces;*
>
> b. *Information, communications and other services, including electronic services and emergency services.*

Article 19 of the CRPD provides for the right to living independent and being included in the community. It states:

> *States Parties to this Convention recognize the equal right of all persons with disabilities to live in the community, with choices equal to others, and shall take effective and appropriate measures to facilitate full enjoyment by persons with disabilities of this right and their full inclusion and participation in the community, including by ensuring that:*
>
> a. *Persons with disabilities have the opportunity to choose their place of residence and where and with whom they live on an equal basis with others and are not obliged to live in a particular living arrangement;*
>
> b. *Persons with disabilities have access to a range of in-home, residential and other community support services, including personal assistance necessary to support living and inclusion in the community, and to prevent isolation or segregation from the community;*
>
> c. *Community services and facilities for the general population are available on an equal basis to persons with disabilities and are responsive to their needs.*

The Rules promote these rights by giving effect to the key safeguards in the Digital ID Act aimed at promoting the enjoyment of rights by persons with disabilities. These safeguards apply in addition to the *Disability Discrimination Act 1992*, which prohibits discrimination

against people on the grounds of disability in employment, education and provision of goods and services.

MEASURES TO MINIMISE THE INTERFERENCE WITH THE RIGHTS OF PERSONS WITH DISABILITIES TO HAVE EQUAL CHOICES

Persons with disabilities can face barriers to create and use a digital ID. The Rules prescribe accessibility and usability requirements to protect and promote the rights of persons with disabilities to have equal access to the benefits of digital ID.

The Rules contain user experience and accessibility requirements that must be met for an entity to become and remain accredited. These requirements will enhance the digital ID experience of persons with disabilities by:

- Requiring accredited entities to comply with accessibility standards or guidelines such as the Web Content Accessibility Guidelines, which are a publication by the Web Accessibility Initiative of the World Wide Web Consortium. This ensures persons with disabilities will have access to simple and easy to understand information about accredited services and enhances their right to choice of a digital ID provider.
- Requiring accredited entities to conduct useability testing with a diverse range of individuals. This provides assurances to the Digital ID Regulator that the entity has taken reasonable steps to ensure its accredited services are accessible to diverse cohorts, including persons with disabilities. Additionally, the testing can help an accredited entity see how diverse cohorts are supported by its services and how to improve these services.
- Requiring accredited entities to have processes or procedures for individuals to make complaints, resolve disputes and receive feedback. This enhances the rights of persons with disabilities as they can offer suggestions to improve accessibility and encourage an accredited entity to continuously improve the accessibility of its services.

MEASURES TO ENSURE PERSONS WITH DISABILITIES CAN PARTICIPATE INDEPENDENTLY

The accessibility requirements contained in Part 4.4 of Chapter 4 of the Rules will enhance the digital ID experience of persons with disabilities and ensure they can participate independently.

The Rules strengthen the right of persons with disabilities to participate independently by:

- Requiring the public-facing information of an accredited entity to be presented in a clear and simple manner. This ensures persons with disabilities can make informed choices about their digital ID.
- Requiring the public-facing information to be available in multiple accessible formats.
- Providing for alternate proofing processes in Rule 5.23 to ensure all individuals can choose to create a digital ID in situations where they do not have, or are unable to obtain, the documents or credentials required to create a digital ID at the identity proofing level sought by the individual. This may enhance the rights of persons with disabilities where they can use alternative forms of documentation (other than driver licence, birth certificate or passport) to create a digital ID.

- Prescribing requirements for accredited entities to provide assisted digital support to users who are unable to use technology independently and inform them of available support. This protects the rights of persons with disabilities as they will be made aware that support is available and can be accessed if they need it.

THE RIGHTS OF EQUALITY AND NON-DISCRIMINATION

Article 26 of the ICCPR states:

> *All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.*

Article 2 of the CROC contains a similar right.

The Rules promote the right to equality and non-discrimination by prescribing requirements relating to accessibility and useability, such as paragraph 3.12(2)(b) which requires an accredited entity to conduct useability testing involving a range of individuals covering diversity in disability, age, gender and ethnicity.

In particular, subrule 4.50(5) helps to ensure that an accredited entity's biometric testing is conducted in accordance with policies covering the ethical use of biometric information and its biometric systems do not disadvantage or discriminate against any group of individuals. Where they are authorised to retain biometric information for testing purposes, accredited entities are required to take reasonable steps to continuously improve their biometric systems to ensure they do not selectively disadvantage or discriminate against any group of individuals. In this way, the Rules help to ensure that these technologies do not pose unintentional barriers to accessibility of digital services for vulnerable groups of people and protect the rights to equality and non-discrimination before the law.

Conclusion on overall compatibility with human rights

The Rules are compatible with human rights, because they promote or positively engage human rights and, to the extent that they may limit human rights, those limitations are reasonable, necessary and proportionate.

Senator the Hon Katy Gallagher, Minister for Finance