EXPOSURE DRAFT

Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025

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

Dated

Katy Gallagher **DRAFT ONLY—NOT FOR SIGNATURE**
Minister for Finance

Consultation draft

Contents

Consultation draft

1 Name

This instrument is the *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025*.

2 Commencement

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

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument	The day after this instrument is registered.	

Note: This table relates only to the provisions of this instrument as originally made.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

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

3 Authority

This instrument is made under section 168 of the *Digital ID Act 2024*.

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

Consultation draft

Schedule 1—PSPF amendments

Digital ID (Accreditation) Rules 2024

1 Subrule 1.4(2)

Insert:

non-corporate Commonwealth entity has the same meaning as in the *Public Governance, Performance and Accountability Act 2013.*

2 Subrule 1.4(2) (definition of *protective security framework*)

Repeal the definition, substitute:

protective security framework means:

(a) the PSPF; or

(b) ISO/IEC 27001; or

(c) an alternative framework (see rule 4.5).

3 Subrule 1.4(2)

Insert:

protective security framework control means:

(a) a relevant PSPF control; or

(b) a control specified in ISO/IEC 27001; or

(c) a control specified in an alternative framework (see rule 4.5).

4 Subrule 1.4(2) (note 1 and note 2 to the definition of *PSPF*)

Repeal the notes, substitute:

Note 1: The PSPF could in 2025 be accessed at https://www.protectivesecurity.gov.au.

Note 2: At the time rule 1.7A commenced, the current version of the PSPF was the PSPF published on 24 July 2025.

5 Subrule 1.4(2)

Insert:

relevant PSPF control: see rule 4.3.

6 Subrule 1.7(2)

Repeal the subrule, substitute:

(2) Unless the contrary intention appears in these rules, an accredited entity is not required to comply with:

(a) a change to the PSPF made after this subrule commences until 3 months after that change has taken effect; and

(b) a change to any other incorporated instrument until 12 months after that change to the incorporated instrument has taken effect.

Note 1: See subsection 167(3) of the Act.

Consultation draft

Note 2: At the time this subrule commenced, the current version of the PSPF was the PSPF published on 24 July 2025.

7 After rule 1.7

Insert:

1.7A Modifications of the PSPF

For the purposes of the incorporation or application of the PSPF by these rules, the PSPF is subject to the following modifications:

(a) a reference to Australian Government resources or Australian Government people and resources in the PSPF is taken to be a reference to DI data environment (within the meaning of these rules);

(b) a reference to risk in the PSPF is taken to be a reference to cyber security risk (within the meaning of these rules).

1.7B Modifications of ISO/IEC 27001

For the purposes of the incorporation or application of ISO/IEC 27001 by these rules, that standard is subject to the following modifications:

(a) a reference to Personally Identifiable Information in the standard is taken to be a reference to personal information (within the meaning of the Act);

(b) a reference to information security incident in the standard is taken to be a reference to cyber security incident (within the meaning of the Act);

(c) a reference to information security risk in the standard is taken to be a reference to cyber security risk (within the meaning of these rules).

8 Subparagraph 3.3(1)(a)(i)

Repeal the subparagraph, substitute:

(i) compliance with the protective security framework controls it complies with, or will comply with if accredited, for the purposes of rule 4.2;

9 Subparagraph 3.3(1)(a)(iii)

Omit “Division 2”, substitute “Division 3”.

10 Subrule 3.5(1)

Omit “a particular protective security control in the framework it implements”, substitute “a particular protective security framework control”.

11 Subrule 3.5(1)

Omit “implement”, substitute “comply with”.

12 Subparagraph 3.5(1)(c)(i)

Omit “implementing the requirement”, substitute “complying with the control or strategy”.

13 Subrule 3.5(2)

Omit “implemented”, substitute “complied with”.

Consultation draft

14 Division 2 of Part 4.1 of Chapter 4 (heading)

Repeal the heading, substitute:

Division 2—Protective security framework controls

15 Rules 4.2 to 4.4

Repeal the rules, substitute:

4.2 Accredited entities must comply with protective security framework controls

(1) An accredited entity must comply, in respect of its accredited services and DI data environment, with either:
  (a) all of the controls specified in ISO/IEC 27001 in accordance with that standard; or
  (b) the controls of an alternative framework in accordance with rule 4.5.

(2) However, if an accredited entity is a non-corporate Commonwealth entity, the entity must comply, in respect of its accredited services and DI data environment, with the relevant PSPF controls in accordance with the PSPF.

(3) This rule applies subject to rule 4.6.

4.3 Relevant PSPF controls

Each of the requirements in the PSPF mentioned in the following table is a ***relevant PSPF control***:

Relevant PSPF controls

Item	The requirements
1	requirement 0007
2	requirement 0008
3	requirement 0009
4	requirement 0010
5	requirement 0014
6	requirement 0017
7	requirement 0018
8	requirement 0019
9	requirement 0020
10	requirement 0021
11	requirement 0022
12	requirement 0023
13	requirement 0024
14	requirement 0025
15	requirement 0026
16	requirement 0036
17	requirement 0037

Consultation draft

Relevant PSPF controls	
Item	**The requirements**
18	requirement 0038
19	requirement 0039
20	requirement 0040
21	requirement 0041
22	requirement 0042
23	requirement 0044
24	requirement 0045
25	requirement 0054
26	requirement 0062
27	requirement 0071
28	requirement 0073
29	requirement 0074
30	requirement 0084
31	requirement 0086
32	requirement 0087
33	requirement 0097
34	requirement 0115
35	requirement 0116
36	requirement 0117
37	requirement 0120
38	requirement 0129
39	requirement 0130
40	requirement 0131
41	requirement 0134
42	requirement 0164
43	requirement 0177
44	requirement 0181
45	requirement 0182
46	requirement 0185
47	requirement 0186
48	requirement 0200
49	requirement 0201
50	requirement 0202
51	requirement 0203

16 Subrules 4.5(1) to (3)

Repeal the subrules, substitute:

(1) An accredited entity (other than a non-corporate Commonwealth entity) may only comply with the controls of an alternative framework if the entity

Consultation draft

demonstrates, in accordance with subrule (2), that the entity complies with all the same kinds of controls specified in ISO/IEC 27001.

(2) To demonstrate that the accredited entity complies with all the same kinds of controls specified in ISO/IEC 27001, the entity must prepare and maintain an up-to-date document that:

(a) maps all the controls specified in the alternative framework that must be complied with against the controls specified in ISO/IEC 27001; and

(b) if the alternative framework does not require compliance with a particular kind of control in ISO/IEC 27001—specifies that particular control.

17 Subrule 4.5(4)

Omit "If an accredited entity implements an alternative framework for the purposes of rule 4.2", substitute "If an accredited entity complies with the controls of an alternative framework for the purposes of paragraph 4.2(1)(b)".

18 Paragraph 4.5(4)(a)

Omit ", and manage and monitor".

19 Subparagraph 4.5(4)(a)(ii)

Omit "or (3)(b)", substitute "of this rule".

20 Subrule 4.5(6)

Repeal the subrule.

21 Rule 4.6

Omit "a particular control in the framework it implements", substitute "a particular protective security framework control".

22 Rule 4.9 (note)

Repeal the note.

23 Subrule 4.12(2)

Repeal the subrule, substitute:

(2) If an accredited entity complies with the relevant PSPF controls for the purposes of rule 4.2:

(a) the entity's system security plan is the security plan referred to in section 3.1 of the PSPF (which deals with security planning); and

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

24 Subrule 4.12(3)

Omit "If an accredited entity implements ISO/IEC 27001", substitute "If an accredited entity complies with ISO/IEC 27001 for the purposes of rule 4.2".

25 After Chapter 7

Insert:

Consultation draft

Chapter 8—Application, saving and transitional provisions

8.1 Transitional provision for amendments made by Schedule 1 to the *Digital ID (Accreditation) Amendment (PSPF and Other Measures) Rules 2025*

(1) This rule applies to an application for accreditation made, but not finally determined, before the commencement day.

(2) Despite the amendments made by Schedule 1 to the amending instrument, the old rules continue to apply on or after the commencement day in relation to that application, as if those amendments had not been made.

(3) In this rule:

amending instrument means the *Digital ID (Accreditation) (PSPF and Other Measures) Amendment Rules 2025.*

commencement day means the day on which this rule commences.

old rules means these rules as in force immediately before the commencement day.

26 Schedule 5

Repeal the Schedule.

Consultation draft

Schedule 2—Duration of consent

Digital ID (Accreditation) Rules 2024

1 Paragraph 4.41(3)(d)

Repeal the paragraph, substitute:

(d) either:

(i) if the accredited entity is an ASP and the individual declares in their consent that their use of the entity's accredited services is for or on behalf of a business (including a business carried on by that individual)—7 years after the consent was initially given; or

(ii) otherwise—12 months after the consent was initially given.

Consultation draft

Schedule 3—Suspension and resumption

Digital ID (Accreditation) Rules 2024

1 Subrule 1.8(1)

Omit "starting on the day that is 12 months after the day on which these rules commence", substitute "on and after 30 November 2025".

2 Subrule 1.8(1) (table items 11 and 12)

Repeal the items.

3 After subrule 1.8(1)

Insert:

(1A) Rule 5.7 and subrule 5.9(2) apply to a transitioned accredited entity on and after 30 November 2026.

4 Subrule 1.8(2)

Omit "subrule (1)", substitute "subrules (1) or (1A)".

Consultation draft