Australian Government
Digital Transformation Agency

07 – Annual Assessment

Trusted Digital Identity Framework Release 4
January 2021, version 1.1

PUBLISHED VERSION

dta

Digital Transformation Agency (DTA)

Licence

Use of the Coat of Arms

The terms under which the Commonwealth Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Conventions

References to TDIF documents, abbreviations and key terms (including the words *MUST*, *MUST NOT*, and *MAY)* are denoted in italics are to be interpreted as described in the current published version of the *TDIF: 01 – Glossary of Abbreviations and Terms.*

TDIF requirements and references to *Applicants* are to be read as also meaning *Accredited Participants*, and vice versa. The scope of *TDIF* requirements are to be read as applying to the identity system under *Accreditation* and not to the organisation's broader operating environment.

Contact us

The *DTA* is committed to providing web accessible content wherever possible. This document has undergone an accessibility check however, if you are having difficulties with accessing the document, or have questions or comments regarding the document please email the Director, Digital Identity Policy at identity@dta.gov.au.

Document management

The *DTA* has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.1	Oct 2019	SJP	Initial version
0.2	Dec 2019	SJP	Updated to incorporate feedback provided by stakeholders during the second round of collaboration on TDIF Release 4
0.3	Mar 2020	SJP	Updated to incorporate feedback provided during the third consultation round on TDIF Release 4
1.0	May 2020		Published version
1.1	Jan 2021	JK	CRID0005 – Emergency Change - ANNUAL-02-05-02 o), and p) referenced requirements that did not exist. Corrected.

Document review

The next scheduled review of this document will occur by July 2022. Any changes made to the document prior to this date will be recorded in a *TDIF* change management document and published to the *DTA* website.

Contents

List of Figures

1 Introduction

This document defines the *TDIF Annual Assessment* process and requirements to be met by an *Accredited Participant* to ensure the *Accredited Participant's* identity system continues to meet the requirements of the *TDIF*. This includes the requirement for an *Accredited Participant* to complete an *Annual Assessment* by the anniversary of its initial accreditation date and provide the resulting *Annual Assessment Report* to the *DTA* for consideration. Failure by an *Accredited Participant* to complete the *Annual Assessment* in accordance with the *TDIF* is a breach of the *Accredited Participant's* obligations under the *TDIF* and may result in the termination of accreditation.

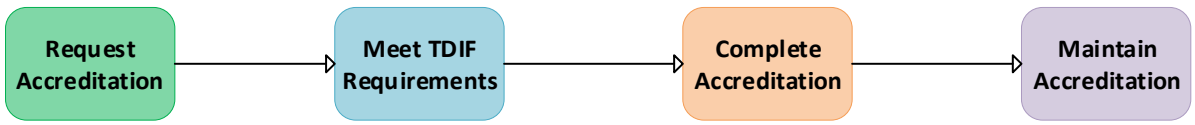
The intended audience for this document includes:

- *Accredited Participants.*
- *Applicants*.
- *Assessors.*
- *Relying Parties*.

1.1 Scope

The *TDIF Accreditation Process* includes four major activities as shown in Figure 1 below. The fourth accreditation activity, 'Maintain Accreditation' is the focus of this document. The three accreditation activities, 'Request Accreditation, Meet TDIF Requirements' and 'Complete Accreditation' are covered in *TDIF: 03 – Accreditation Process*.

Figure 1: TDIF Accreditation Process.



2 Maintain TDIF accreditation

To maintain *TDIF* accreditation, the *Accredited Participant* is required to undergo an *Annual Assessment* by suitably skilled, independent and experienced *Assessors*.

2.1 Previous Functional Assessments

The *Accredited Participant* may have recently undergone assessments on its identity system which cover similar requirements to those listed in the *TDIF*. The *Accredited Participant* may submit evidence of these assessments conducted in the previous 12 months and request the *DTA* consider it as a suitable substitute for an *Annual Assessment* requirement.

At its discretion, the *DTA* may accept prior assessments conducted on the *Accredited Participant's* identity system as a substitute to an *Annual Assessment* requirement required by the *TDIF*. In such instances the *DTA* will advise the *Accredited Participant* in writing the adequacy of prior assessments relative to the degree to which they cover *TDIF* requirements. Where the *DTA* determine a prior assessment:

- Fully addresses an *Annual Assessment* requirement then no further action will be required by the *Accredited Participant* for that requirement.
- Partially addresses an *Annual Assessment* requirement then the *Accredited Participant* will need to undergo a partial *Annual Assessment* for the requirements it does not meet.
- Does not address an *Annual Assessment* requirement then the *Accredited Participant* will need to meet the requirement as listed in the *TDIF*.

2.2 Accredited Participant obligations

TDIF Req: ANNUAL-02-02-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Accredited Participant* *MUST* ensure that all *Annual Assessment* requirements are completed by the anniversary of its initial accreditation date. Failure by an *Accredited Participant* to complete the *Annual Assessment* in accordance with the *TDIF* is a breach of the *Accredited Participant's* obligations under the *TDIF* and may result in the termination of accreditation.

2.3 Assessor skills, experience and independence

TDIF Req: ANNUAL-02-03-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Accredited Participant* *MUST* demonstrate to the *DTA* how the *Assessors* have relevant, reasonable and adequate experience, training and qualifications to conduct the *Annual Assessment*.

TDIF Req: ANNUAL-02-03-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Accredited Participant* *MUST* demonstrate to the *DTA* how the *Assessors*:

- Are independent from the development and operational teams of the *Accredited Provider's* identity system.
- Do not possess a conflict of interest in performing the *Annual Assessment* on the *Accredited Participant's* identity system.

2.4 Annual Assessment schedule

TDIF Req: ANNUAL-02-04-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

Annual Assessments that occur during:

- Even calendar years (i.e. 2020, 2022, 2024, etc) *MUST* be undertaken by *Assessors* who are external to the *Accredited Participant's* organisation.
- Odd calendar years (i.e. 2021, 2023, 2025, etc) *MAY* be undertaken by *Assessors* who are external to the development and operational teams of the *Accredited Provider's* identity system.

2.4.1 Annual Assessment process

TDIF Req: ANNUAL-02-04-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Accredited Participant* *MUST* ensure *Assessors* have access to and consider all relevant evidence provided by the *Accredited Participant* to the *DTA*. This includes any responses by the *DTA* to questions which may have been asked.

TDIF Req: ANNUAL-02-04-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Accredited Participant* *MUST* ensure *Assessors* conduct the *Annual Assessments* and prepares the *Annual Assessment Report* in accordance with the requirements of the *TDIF*.

TDIF Req: ANNUAL-02-04-04; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Accredited Participant* *MUST* use the compliance ratings listed in 'Appendix A: Compliance ratings' when determining areas of compliance and non-compliance with the requirements of the *TDIF*.

TDIF Req: ANNUAL-02-04-05; **Updated**: Mar-20; **Applicability**: A, C, I, X
As part of the *Annual Assessment*, the *Assessors* *MUST* undertake the following activities:

a) Documentation reviews.
b) Interviews with key personnel.
c) A run through of the *Accredited Participant's* identity system.

TDIF Req: ANNUAL-02-04-05a; **Updated**: Mar-20; **Applicability**: A, C, I, X
As part of the *Annual Assessment*, the *Assessors* *MAY* undertake a site visit to the *Accredited Participant's* premises or other location where it provides services in connection with its identity system.

TDIF Req: ANNUAL-02-04-06; **Updated**: Mar-20; **Applicability**: A, C, I, X
As part of the *Annual Assessment* the *Accredited Participant* *MUST* provide the *DTA* with:

a) A copy of all *Annual Assessment Reports* (as per ANNUAL-02-05-01) which include all required information (as per ANNUAL-02-05-04).

b) A response from the *Accredited Participant's Accountable Authority* to all adverse findings identified by the *Assessors* in the *Annual Assessment Reports* (as per ANNUAL-02-05-03).
c) A copy of all decisions and supporting documentation (as per ANNUAL-02-05-02).
d) An annual *Qualifying Attestation Letter* in accordance with the requirements set out in ANNUAL-02-06-01 and ANNUAL-02-06-02.

An executive summary or redacted version of this information is insufficient to meet this requirement.

The *DTA* will acknowledge receipt of the *Annual Assessment Reports*, *Qualifying Attestation Letter,* decisions and supporting documentation and conduct a review of the documents. Once this review is completed, the *DTA* will advise the *Accredited Participant* of its acceptance of the documents and whether they meet *TDIF* requirements. This includes whether the proposed remediation actions, and timings, are acceptable[1]. The *Accredited Participant* ***MUST*** remediate any non-compliances or adverse findings to the satisfaction of the *DTA* within agreed timeframes.

2.5 Annual Assessment reporting

TDIF Req: ANNUAL-02-05-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Accredited Participant* ***MUST*** ensure that the *Assessor* prepares *Annual Assessment Reports* which cover:

a) The *Privacy Assessment* (as per ASSESS-07-01-04).
b) The security assessment (as per ASSESS-07-02-01).
c) The penetration test (as per ASSESS-07-02-02).
d) An annual usability test (as per UX-05-05-02)
e) An assessment against the *Web Content Accessibility Guidelines* (as per ASSESS-07-03-01).

TDIF Req: ANNUAL-02-05-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

[1] If the proposed remediation actions are not acceptable, the *DTA* will advise the *Accredited Participant* accordingly, state the reasons why the actions are not accepted, and what the *Accredited Participant* will need to do in order for its proposed remediation actions to be acceptable.

As part of the *Annual Assessment* the *Accredited Participant* *MUST* provide the *DTA* with:

a) Any decisions and supporting documentation made by the *Accredited Participant's Accountable Authority* to vary its fraud control arrangements during the year (as per FRAUD-02-01-03).
b) Evidence the *Accredited Participant* has reviewed its *Fraud Control Plan* (and supporting *Fraud Control Plans*) during the year (as per FRAUD-02-02-02).
c) A copy of fraud awareness training materials provided by the *Accredited Participant* to *Personnel* during the year (as per FRAUD-02-03-01).
d) Evidence of the *Accredited Participant* has reviewed its *Privacy Policy* and where relevant updated during the year (as per PRIV-03-02-05).
e) Evidence of the *Accredited Participant* has reviewed its *Privacy Management Plan* and where relevant updated during the year (as per PRIV-03-02-07).
f) A copy of privacy awareness training materials provided by the *Accredited Participant* to *Personnel* during the year (as per PRIV-03-02-08).
g) For *Identity Exchanges*, a copy of their *Annual Transparency Report* (as per PRIV-03-06-05).
h) Any decisions and supporting documentation made by the *Accredited Participant's Accountable Authority* to vary its protective security control arrangements during the year (as per PROT-04-01-03).
i) A copy of protective security training materials provided by the *Accredited Participant* to *Personnel* during the year (as per PROT-04-01-07).
j) Evidence of the *Accredited Participant* has reviewed its *System Security Plan* (and supporting *System Security Plans*) and where relevant updated during the year (as per PROT-04-01-13).
k) Any decisions and supporting documentation made during the year by the *Accredited Participant's Chief Security Officer* (or their delegate) to implement alternative mitigation measures or controls to those listed in the *TDIF* protective security requirements (as per PROT-04-01-18).
l) Evidence the *Accredited Participant* has tested its *Disaster Recovery and Business Continuity Plan* during the year (as per PROT-04-02-27).
m) Outcomes of its annual usability test conducted on its identity system (as per UX-05-05-04a).
n) For *Identity Service Providers*, processes and risk assessments to support exception cases (as per IDP-03-03-01b)

o) For *Identity Service Providers*, the evaluation, results and report for the presentation attack detection technology used (as per IDP-03-08-10b).
p) For *Identity Service Providers*, a copy of *Manual Face Comparison* training materials provided to *Personnel* during the year (as per IDP-03-08-23).
q) For *Attribute Service Providers*, evidence of its arrangements with an Authoritative Source (as per ASP-05-02-01a)
r) Where an *Accredited Participant* has been granted an exemption against a *TDIF* requirement, justification the exemption is still required. (The *TDIF* exemption process is set out in B.2 of the *TDIF: 03 Accreditation Process*).

TDIF Req: ANNUAL-02-05-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Accredited Participant's Accountable Authority* MUST respond in writing to any adverse findings identified by the *Assessors* in the *Annual Assessment Reports* including whether the recommendations are accepted, the reasons for any non-acceptance and the timeframe for implementation of the recommendations.

TDIF Req: ANNUAL-02-05-04; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Annual Assessment Reports* MUST include the following:

a) The date of and period covered by the report.
b) Name, role (or position) and contact details of the relevant *Accountable Authority* and point of contact within the *Accredited Participant's* organisation.
c) Qualifications and basis of independence for all *Assessors* used.
d) Names and version numbers of all documents used by the *Accredited Participant*.
e) City, state and (if applicable) country of all physical locations used in the *Accredited Participant's* operations. This includes data centre locations (primary and alternative sites) and all other locations where general *ICT* and business process controls that are relevant to the *Accredited Participant's* operations are performed.
f) The test or evaluation methodology(s) used.
g) The test or evaluation results.
h) Findings.
i) Remediation actions or recommendations to address any areas of non-compliance.
j) Express an opinion and provide recommendations to the *DTA* of the *Accredited Participant's* identity system against the *TDIF* requirements,

including any requirements that could not be adequately assessed due to access or timing issues.

k) Include a list of compliant and non-compliant controls.

l) Where a non-compliance has been identified, the remedial actions and timeframes within which actions will be completed to address the non-compliance.

2.6 Qualifying Attestation Letter

TDIF Req: ANNUAL-02-06-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Qualifying Attestation Letter* *MUST*, at a minimum, contain information that supports the *Accredited Participant's* claim that its operations remain in accordance with *TDIF* requirements.

TDIF Req: ANNUAL-02-06-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
In addition, the *Qualifying Attestation Letter* *MUST* be signed by the *Accredited Participant's* relevant *Accountable Authority* and include the name, role/position and contact details of the *Accountable Authority* that is asserting that the *Accredited Participant's* identity system complies with TDIF requirements.

TDIF Req: ANNUAL-02-06-03; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Accredited Participant* *MAY* publish the *Qualifying Attestation Letter* onto its public dashboard or website.

2.7 TDIF Reaccreditation

Threat environments and business needs are dynamic. While regular accreditation activities are highly beneficial in maintaining the trust posture of the *Accredited Participant's* identity system, other activities may necessitate a need for *TDIF Reaccreditation* outside of regularly scheduled timeframes. This may include:

- Changes in information security policies.
- Detection of new or emerging threats to systems.
- The discovery that security measures are not operating as effectively as planned.
- The occurrence of a reportable incident (security, privacy or fraud).

- Architectural changes to the system.
- Changes to the system risk profile.
- Changes to an agency's risk appetite, ICT resourcing or senior support.
- Changes to physical locations.
- Changes in ownership.

In addition to meeting ongoing *TDIF* accreditation obligations, an *Accredited Participant* may be directed by the *DTA* to undergo *TDIF Reaccreditation*. This will occur if the *Accredited Participant's* identity system is changed in a manner that may result in:

- Significant impacts to the *Accredited Participant's* protective security arrangements.
- Serious or repeated privacy breaches (including of *TDIF* requirements or the *Australian Privacy Principles*).
- Material changes to the *Accredited Participant's* risk exposure.
- Material changes to the risk exposure of other *Accredited Participants* in the *Australian Government's identity federation* that materially impact the *Accredited Participant*.
- After a significant change to the *Accredited Participant's identity system* that significantly impacts on the agreed and implemented system architecture and *System Security Plan*.
- After significant changes to the threats or risk faced by the *Accredited Participant's* identity system.

In such circumstances, the *DTA* will outline the *TDIF Reaccreditation* requirements to be met in writing. The costs associated with these requirements are to be met by the *Accredited Participant* and will not replace their annual compliance obligations.

To assist in the *TDIF Reaccreditation* of an identity system, *Accredited Participants* are encouraged to reuse as much information from previous *Annual Assessments* as possible.

Accredited Participants that fail to complete *TDIF Reaccreditation* as directed by the *DTA* represents a breach of the *TDIF* and may result in the termination of accreditation.

Appendix A: Compliance ratings

Assessors must use the following compliance ratings to indicate whether the *Accredited Participant's* identity system continues to meet *TDIF* requirements. Refer to the ISO 31000 or the *Accredited Participant's* own risk management framework for a description of likelihood and consequence ratings.

- **Not Applicable (N/A)**. A TDIF requirement that does not apply to an *Accredited Participant* as their identity system does not use, rely on or support the *TDIF* requirement (for example, *TDIF* requirements for elliptic curve cryptography will be N/A if the identity system supports other approved cryptographic algorithms instead).
- **Compliant**. The *Accredited Participant* has demonstrated with evidence they comply with a *TDIF* requirement or the intent of a requirement.
- **Critical Non-Compliance**. The *Accredited Participant* fails to meet a *TDIF* requirement which may result in extreme unmitigated risk.
    - A critical non-compliance must be classified as such and must result in a failed *Annual Assessment*.
    - The immediate withdrawal of an existing *TDIF* accreditation by the DTA may occur until such time as the critical non-conformance is sufficiently mitigated.
- **Major Non-Compliance**. The *Accredited Participant* fails to meet a *TDIF* requirement which may result in high unmitigated risk.
    - A major non-compliance must be classified as such and must result in a failed *Annual Assessment*.
    - Escalation of the problem to a critical failure must be imposed if additional failures within this category are detected.
    - If the *Accredited Participant* fails to rectify the compliance problem within a timeframe agreed with the *DTA*, then the status of the problem must be escalated to a critical failure and the conditions of that category are then applied.
- **Partial Non-Compliance**. The *Accredited Participant* fails to meet a *TDIF* requirement which may result in moderate unmitigated risk must be classified as a partial failure.
    - Escalation of the problem to a major failure must be imposed if additional failures within this category are detected.

- If the *Accredited Participant* fails to rectify the compliance problem within a timeframe agreed with the *DTA*, then the status of the problem must be escalated to a major failure and the conditions of that category are then applied.

- **Minor Non-Compliance**. The *Accredited Participant* fails to meet a *TDIF* requirement which may result in low unmitigated risk should be classified as minor failures.
  - Escalation of the problem to a partial failure must be imposed if additional failures within this category are detected.
  - If the *Accredited Participant* fails to rectify the compliance problem within a timeframe agreed with the *DTA*, then the status of the problem must be escalated to a partial failure where the conditions of that category are then applied.