Australian Government

Digital Identity

07 Maintain Accreditation

Trusted Digital Identity Framework

Release 4.6 - March 2022

PUBLISHED VERSION

Digital Transformation Agency (DTA)

Licence

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 Providers*, and vice versa. The scope of *TDIF* requirements are to be read as applying to the *Accredited Provider* undergoing *Annual Accreditation*, including, where relevant, the *Accredited Provider*'s *Identity System,* 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

Document Version	Release 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	4.0	May 2020		Published version
1.1	4.1	Jan 2021	JK	CRID0005 – Emergency Change - ANNUAL02-05-02 o), and p) referenced requirements that did not exist. Corrected.
1.2	4.4	June 2021	JK	CRID0001 - Defined terms update to requirements.
1.3	4.6	Feb 2022	JK, AV, MS, DN, SJP	Applicability of requirements added. Improvements to structure and clarity. Guidance updated. See TDIF Change Log for full list and description of changes

All changes made to the TDIF are published in the TDIF Change Log which is available at https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework.

Contents

List of Figures

1 Introduction

This document defines the *TDIF Annual Assessment* process and requirements to be met by an *Accredited Provider* to ensure the *Accredited Provider* and *the Accredited Provider's Identity System* continue to meet the requirements of the *TDIF*.

This includes the requirement for an *Accredited Provider* to provide its *Annual Assessment Reports,* supporting documentation, and any other information to the *DTA* for consideration by the anniversary of its initial accreditation date in order to complete its *Annual Assessment*. Failure by an *Accredited Provider* to complete the *Annual Assessment* in accordance with the *TDIF* is a breach of the *Accredited Provider's* obligations under the *TDIF* and may result in the suspension or termination of accreditation.

The intended audience for this document includes:

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

1.1 Scope

The *TDIF Accreditation Process* includes five major activities as shown in Figure 1 below. The fifth accreditation activity, 'Maintain Accreditation' is the focus of this document. The other four accreditation activities, 'Preliminary Preparations', '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 Provider* is required to undergo an *Annual Assessment,* which includes:

- An assessment against all applicable requirements in *TDIF 07 Maintain Accreditation,*
- commissioning suitably skilled, independent and experienced *Assessors* to conduct *Functional Assessments, and*
- if applicable, undergo a *Usability Test* or *Biometric Testing*.

Accredited Providers should be aware of the following terms used throughout this document:

- **Annual Assessment** – meaning the DTA's assessment of the *Accredited Provider's* compliance with all the *TDIF 07 Maintain Accreditation document.*
- **Functional Assessment** – Assessments of an *Applicant's Identity System* by an *Assessor* to establish conformance with applicable TDIF Requirements. An *Assessor* prepares a *Functional Assessment* report on the outcomes of their assessment.
- **Annual Assessment Report** – a full report on each *Functional Assessment* which the *Accredited Provider* must prepare. Each annual assessment report submitted to the DTA includes the *Assessor's Functional Assessment* report and the responses from *the Accredited Provider's Accountable Executive* on risks or non-compliances the *Assessor* has identified in their *Functional Assessment* report.

A full list of all supporting documentation and information required to be submitted to the DTA as evidence of the *Accredited Provider's* accreditation activities is in **Appendix B**.

2.1 Accredited Provider ongoing obligations

Accredited Providers are required to meet all ongoing obligations outlined in the *TDIF Agreement (MOU)*. This includes continuing to meet all applicable TDIF requirements its accredited *Identity System* has been assessed against as part of the initial accreditation.

In addition to the *Accredited Provider's Functional Assessments*, testing and other required supporting documentation, the DTA may request supplementary evidence that an *Accredited Provider* continues to meet the TDIF requirements.

TDIF Req: ANNUAL-02-01-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
If the DTA requests evidence that an *Accredited Provider* continues to meet a TDIF requirement, the *Accredited Provider* ***MUST*** provide this evidence as part of its Annual Assessment.

TDIF Req: ANNUAL-02-01-01a; **Updated**: Mar-22; **Applicability**: A, C, I, X
Accredited Providers ***MUST*** meet any new or amended requirements in the newest version of the TDIF, published on the TDIF website, within 12 months of that version being published. These requirements will be assessed as part of the *Accredited Provider's Annual Assessment.*

NOTE: If an *Accredited Provider* does not provide the information required by ANNUAL-02-01-01 or ANNUAL-02-01-01a by their Annual Assessment date, the DTA will then assess whether the *Accredited Provider* has failed to meet one or more of their ongoing obligations. If the DTA finds that the *Accredited Provider* has failed to meet their obligations, this will result in a finding of non-compliance with the TDIF. A finding of non-compliance may result in a failed Annual Assessment. A failed Annual Assessment may result in suspension or termination of accreditation.

TDIF Req: ANNUAL-02-01-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
If the DTA makes a finding that the *Accredited Provider* has failed to comply with ANNUAL-02-01-01 and ANNUAL-02-01-01a, the DTA will advise the *Accredited Provider* of the non-compliance in writing and direct it to submit evidence to meet the relevant requirements. The *Accredited Provider* ***MUST*** provide to the DTA in writing:

a) a risk rating assigned to each instance of non-compliance as set out in **Appendix A**; and
b) Include details of:
    i. each such risk assessment;
    ii. A copy of the *Accredited Provider's* risk matrix; and
    iii. a description of the likelihood and risk categories associated with the risk ratings assigned above.

TDIF Req: ANNUAL-02-01-02a; **Updated**: Mar-22; **Applicability**: A, C, I, X
Any risks or recommendations identified in ANNUAL-02-01-02 *MUST NOT* meet or exceed a High or Extreme risk rating[1] for the *Accredited Provider's Annual Assessment.*

TDIF Req: ANNUAL02-01-02b; **Updated**: Mar-22; **Applicability**: A, C, I, X
If the risk rating meets or exceeds that outlined above in ANNUAL-02-01-02a, the *Accredited Provider MUST* confirm:

a) it has implemented mitigations to address the recommendation, risk or non-compliance
b) The risk, recommendation or non-compliance has been reassessed and the residual risk rating is at Moderate or below; and
c) The *Accountable Executive* has signed off and confirmed the implemented mitigation of the risk and the new residual risk rating.

NOTE: If the *Accredited Provider* cannot meet ANNUAL-02-01-02a, then this will result in a failed Annual Assessment. Where the DTA makes a finding that an *Accredited Provider* has failed an Annual Assessment, the DTA will make a decision whether the *Accredited Provider*'s accreditation will be suspended or terminated.

2.1.1 Changes to an Accredited Provider's Identity System

TDIF Req: ANNUAL-02-01-03; **Updated**: Mar-22; **Applicability**: A C, I, X
If an *Accredited Provider*'s *Identity System* releases a *Major Production Release*, or is changed or impacted in such a manner, that results in:

- Significant impacts to the *Accredited Provider's* protective security arrangements
- Serious or repeated privacy breaches (including of *TDIF* requirements or the *Australian Privacy Principles*)
- Material changes to the *Accredited Provider's* risk exposure where such exposure results in the Applicant identifying High or Extreme risks (as per Appendix A – Risk Ratings or the *Accredited Provider*'s own equivalent risk framework)

[1] According to Appendix A in TDIF 07 Maintain Accreditation, or the Applicant's equivalent risk framework.

- A significant change to the *Accredited Provider's Identity System* that significantly impacts on the agreed and implemented system architecture and *System Security Plan*
- significant changes to the threats or risk faced by the *Accredited Provider's Identity System*, or
- TDIF requirements that were not previously applicable to an *Accredited Provider*'s *Identity System* becoming applicable[2]

then *the Accredited Provider* ***MUST*** inform the DTA of changes to their *Identity System* as part of its Annual Assessment and any provisions as stipulated by the TDIF Agreement (MOU).

The DTA will decide, and provide its decision in writing, whether *the Accredited Provider* will need to formally apply for a Variation in Accreditation or, depending on the severity of risks or impacts to the *Accredited Provider*'s *Identity System*, whether the accreditation should be suspended or terminated.

2.1.2 Variations of Accreditation

An *Accredited Provider* may seek to vary its accreditation in response to changes to its architecture, a new feature implementation, step-up of Identity Proofing or Credential level, or if it is seeking to be accredited for an additional TDIF Role.

A change in architecture or feature implementation is likely to have impacts on other TDIF requirements, such as the *Accredited Provider*'s System Security Plan, Fraud Control Plan and Privacy arrangements and documentation. These circumstances may result in the DTA assessing the *Accredited Provider* for reaccreditation.

The DTA and *Accredited Provider* may undergo a scoping activity to understand which TDIF requirements are affected by the changes to the *Accredited Provider*'s *Identity System*. This scoping activity will assist DTA in determining any additional evidence to be provided to meet the TDIF requirements.

[2] for example, an IDX implementing the User Dashboard feature which would result in section 6.4 of TDIF 05 Role Requirements now being applicable

TDIF Req: ANNUAL-02-01-04; **Updated**: Mar-22; **Applicability**: A, C, I, X
If an *Accredited Provider* seeks to vary its accreditation, it *MUST* complete a *TDIF Application Letter* as per requirements ACCRED-03-01-01 to ACCRED-03-01-05 and the requirements below.

TDIF Req: ANNUAL-02-01-05; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider MUST* submit a *Requirements Traceability Matrix* and identify all applicable TDIF requirements that may be impacted by the variation of accreditation.

NOTE: the DTA will assess the *Requirements Traceability Matrix* and may identify additional applicable requirements that an *Accredited Provider* must submit evidence for.

TDIF Req: ANNUAL-02-01-06; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider MUST* include and submit to the DTA a review of the applicable evidence required for variation of accreditation, **as outlined in Appendix C.**

TDIF Req: ANNUAL-02-01-07; **Updated**: Mar-22; **Applicability**: A, C, I, X
An *Accredited Provider MAY* use *Alternative Assessment Reports* as per requirements ANNUAL-02-03-01 to ANNUAL-02-03-01b to meet the TDIF requirements.

TDIF Req: ANNUAL-02-01-07a; **Updated**: Mar-22; **Applicability**: A, C, I, X
If an *Accredited Provider* submits an *Alternative Assessment Report* as per ANNUAL-02-01-07, then it *MUST* cover the changes to the *Accredited Provider*'s *Identity System*.

2.1.3 TDIF Reaccreditation

TDIF Reaccreditation is a process where an *Accredited Provider* is directed by the DTA to complete accreditation activities in addition to their ongoing obligations to maintain accreditation. It encompasses a review and rescoping of all applicable initial accreditation requirements to assess whether any further evidence statements or

updates to documentation is required in response to the reason the *Accredited Provider* has been directed to complete a Reaccreditation Activity.

Reasons for TDIF Reaccreditation

An *Accredited Provider* may be directed by the *DTA* to undergo *TDIF Reaccreditation* following a cyber security or fraud incident, serious or repeated data or privacy breaches, or as a result of a changing threat or operating environment which materially impacts the *Identity System's* risk profile.

TDIF Reaccreditation may be required if an *Accredited Provider* seeks to vary its accreditation (e.g. accredit a new feature or *Role*).

Reactivation of an *Accredited Provider*'s TDIF Accreditation after a Suspension of Accreditation is also appropriate grounds for the DTA to direct an *Accredited Provider* to undergo a *TDIF Reaccreditation.*

Threat environments and business needs are dynamic. While regular accreditation activities are highly beneficial in maintaining the trust posture of the *Accredited Provider'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).
- Changes to the system risk profile.
- Changes to an agency's risk appetite, ICT resourcing or senior support.
- Changes to physical locations.
- Changes in control or ownership of the *Accredited Provider*'s organisation.

In addition to meeting ongoing *TDIF* accreditation obligations, an *Accredited Provider* may request or be directed by the *DTA* to undergo *TDIF Reaccreditation*.

Undergoing TDIF Reaccreditation

The costs associated with these requirements are to be met by the *Accredited Provider* and the *DTA* will determine whether it replaces the requirement for the *Accredited Provider's Annual Assessment* depending on the extent of requirements

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

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

2.1.4 Suspension of Accreditation

Suspension by the DTA

The DTA may, in writing, suspend the accreditation of an *Accredited Provider* if:

- the DTA reasonably believes that the *Accredited Provider* has breached a TDIF requirement or is contravening the TDIF Agreement (MOU); or
- the DTA reasonably believes there has been a *Cyber Security Incident*, or series of incidents, involving the *Accredited Provider*, which demonstrates a material compromise of the *Accredited Provider's* security; or
- if the entity is a body corporate—the entity becomes a Chapter 5 body corporate (within the meaning of the Corporations Act 2001); or

Before suspending the accreditation of an *Accredited Provider*, the DTA will give a written notice, signed by the Accreditation Authority to the *Accredited Provider:*

- to state the grounds on which the DTA proposes to suspend the *Accredited Provider*'s accreditation; and

- invite the *Accredited Provider* to give the DTA, within 28 business days after the day the notice is given, a written statement showing cause why the DTA should not suspend the accreditation.

The *Accredited Provider* will not receive this notice if the suspension is on the grounds that there has been a *Cyber Security Incident*, or series of incidents, involving the *Accredited Provider*, which demonstrates a material compromise of the *Accredited Provider's* security. If the DTA suspends accreditation on this ground, the DTA will provide written notice to the *Accredited Provider* within 7 days setting out the reasons for the suspension.

If the DTA decides to proceed with suspending the accreditation, it will give written notice to the *Accredited Provider*. This written notice will state the following:

- that the *Accredited Provider*'s accreditation is suspended;
- if the *Accredited Provider* is accredited as more than one role—the accredited role that is suspended;
- the reasons for the suspension;
- the day the suspension is to start;
- if the accreditation is suspended for a period—the period of the suspension;
- if the accreditation is suspended until a specified event occurs or action is taken—the event or action;
- if the accreditation is suspended indefinitely—that fact
- any directions that may be necessary to give effect to the suspension

Suspension at the request of an Accredited Provider

An *Accredited Provider* may also request for that its accreditation to be suspended.

If the *Accredited Provider* applies to the DTA to suspend its accreditation, the *DTA* may suspend the *Accreditation.*

Consequences of suspension of accreditation

Suspension of an *Accredited Provider*'s TDIF Accreditation means that, during any period where the Accreditation is suspended:

- The Status of Accreditation of the *Accredited Provider* on the TDIF website will be changed from "Active" to "Suspended"
- The *Accredited Provider* must cease making any representations, publicly or privately, that it holds an "Active" TDIF Accreditation.

Resolving a Suspension of Accreditation

An *Accredited Provider* may apply to the DTA to revoke the suspension, whether the suspension was at the initiative of the DTA or on request of the *Accredited Provider*.

If the DTA has suspended an *Accredited Provider*'s Accreditation of its own initiative, the *Accredited Provider* must address the reasons that lead to the DTA suspending the accreditation, and may be directed by the DTA to undergo reaccreditation as part of this process.

If the DTA revokes the suspension of an accreditation, it will do so by providing a written notice to the *Accredited Provider*.

2.1.5 Termination of Accreditation

Ceasing to hold Accreditation

Termination of the TDIF Agreement (MOU) by the DTA

In accordance with clause 16 of the *TDIF Agreement (MOU)*, a valid termination of the *TDIF Agreement (MOU)* by the DTA will mean that the *Accredited Provider* ceases to hold *Accreditation*.

The DTA may terminate the *TDIF Agreement (MOU)* for an Event of Default (as defined in clause 13 of the *TDIF Agreement (MOU).*

The process for terminating the *TDIF Agreement (MOU)* is set out in that document, including the steps the DTA will take if relying on an Event of Default.

Termination of the TDIF Agreement (MOU) by the Accredited Provider

An *Accredited Provider* wishing to cease holding accreditation must terminate the TDIF Agreement (MOU) in accordance with its terms.

In accordance with clause 16 of the TDIF Agreement (MOU), a valid termination of the TDIF Agreement (MOU) by the *Accredited Provider* will mean that the *Accredited Provider* cases to hold *Accreditation*.

Consequences of ceasing to hold accreditation

Ceasing to hold TDIF Accreditation means that:

- The Status of Accreditation of the *Accredited Provider* on the TDIF website will be changed from “Active” to “Terminated”
- The *Accredited Provider* must cease making any representations, publicly or privately, that it holds a TDIF Accreditation.
- If the *Accredited Provider* wishes to obtain accreditation again, they must apply for TDIF accreditation as per the TDIF 03 Accreditation Process and go through Initial accreditation.

2.2 Annual Assessment Requirements

TDIF Req: ANNUAL-02-02-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* *MUST* meet all obligations set out in the TDIF Agreement (MOU) and provide evidence of such to the DTA.

TDIF Req: ANNUAL-02-02-02; **Updated**: Mar-22; **Applicability**: A, C, I, X

The *Accredited Provider* *MUST* ensure that all *Annual Assessment* requirements are completed by the anniversary of its initial accreditation date.

NOTE: If the *Accredited Provider* cannot meet ANNUAL-02-02-01 and ANNUAL-02-02-02, then this will result in a failed Annual Assessment. Where the DTA makes a finding that an *Accredited Provider*

has failed an Annual Assessment, the DTA will make a decision whether the *Accredited Provider*'s accreditation will be suspended or *terminate*d.

In order for the *DTA* to review an *Accredited Provider's Annual Assessment* materials, the *Accredited Provider* should submit its Annual Assessment evidence at least two months prior to the anniversary of its initial accreditation date

TDIF Req: ANNUAL-02-02-03; **Updated**: Jun-21; **Applicability**: A, C, I, X
Before the anniversary of the *Accredited Provider's* initial accreditation date, the *Accredited Provider* *MUST* provide the *DTA* with a full and unredacted copy of:

a) each *Functional Assessment* report prepared under ANNUAL-02-07-04.
b) Where applicable, the *Accredited Provider*'s Annual Usability Test Report conducted in accordance with ANNUAL-02-04-02
c) the *Accredited Provider's Annual Assessment Reports* prepared in accordance with ANNUAL-02-08-01
d) each response from the *Accredited Provider's Accountable Executive* under ANNUAL-02-08-02a.
e) All applicable evidence required as part of the review under Section 2.9 Evidence Review Requirements and listed in **Appendix B**.
f) An annual *Qualifying Attestation Letter* in accordance with the requirements set out in ANNUAL-02-02-04.

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,* supporting documentation and evidence and conduct a review of the documents. Once this review is completed, the *DTA* will advise the *Accredited Provider* of its acceptance of the reports and evidence and whether it meets the applicable *TDIF* requirements. This includes whether the proposed remediation actions and timings, are acceptable.

2.2.1 Qualifying Attestation Letter

TDIF Req: ANNUAL-02-02-04; **Updated**: Jun-21; **Applicability**: A, C, I, X
Once the *Accredited Provider* has achieved all applicable TDIF Annual Assessment requirements, it *MUST* submit a *Qualifying Attestation Letter* signed by the *Accredited Provider*'s Accountable Executive that contains the following information

to support the *Accredited Provider's* claim that its operations remain in accordance with *TDIF* requirements:

- The name, role/position and contact details of the *Accountable Executive*
- A statement that the *Accredited Provider's Identity System* complies with the TDIF requirements and the TDIF Agreement (MOU)
- The version of the TDIF the *Accredited Provider* is assessed and accredited under for the relevant Annual Assessment[3]
- a statement confirming it has provided the DTA with all relevant documents, materials and evidence to the accreditation as part of its review
- A statement confirming that the evidence provided is a fair and accurate representation of its *Identity System*
- If the *Accredited Provider* has risks or non-compliances identified in its *Annual Assessment Reports*, then the Qualifying Attestation Letter ***MUST*** contain a summary of these risks, implementation dates and any further information as per ANNUAL-02-08-02 to ANNUAL-02-08-04a

A template for the Qualifying Attestation Letter is available from the TDIF website.

2.3 Alternative Assessment Reports

The *Accredited Provider* may have recently undergone assessments on its Identity System which cover similar requirements to those listed in the TDIF. The *Accredited Provider* 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 as a substitute to an Annual Assessment requirement required by the TDIF.

Further details of the process and requirements for submitting prior assessments are detailed in TDIF: 03 – Accreditation Process (see section 3.2.3 "*Alternative Assessment Report*s Requirements").

[3] An Accredited Provider's obligations to comply with the latest version of the TDIF published on the TDIF website is outlined in the TDIF Agreement (MOU)

The DTA will advise the *Accredited Provider* 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 Provider* for that requirement.
- Partially addresses an Annual Assessment requirement then the *Accredited Provider* 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 Provider* will need to meet the requirement as listed in the TDIF.

TDIF Req: ANNUAL-02-03-01; **Updated**: Jun-21; **Applicability**: A, C, I, X

If an *Accredited Provider* requests that an Alternative Assessment should be considered by the DTA as a substitute for a relevant *Functional Assessment* or as evidence to meet other TDIF requirements, then it *MUST* submit the *Alternative Assessment Report* as per the following requirements.

TDIF Req: ANNUAL-02-03-01a; **Updated**: Jun-21; **Applicability**: A, C, I, X

Any request made to the *DTA* to consider *Alternative Assessment Reports MUST* include:

a) Which *Functional Assessment* or TDIF requirements it is provided as evidence for
b) A rationale for why the *Alternative Assessment Report* should be considered as equivalent to a *Functional Assessment* or as appropriate evidence to meet the TDIF Requirements, and
c) A *Requirements Traceability Matrix*, which sets out:
    i. each TDIF requirement the *Alternative Assessment Report* addresses,
    ii. a reference to where the *Alternative Assessment Report* addresses that TDIF requirement (e.g. page number or section), and
    iii. any supporting statements for why that section of the *Alternative Assessment Report* addresses the TDIF requirements (if needed).

TDIF Req: ANNUAL-02-03-01b; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Alternative Assessment Report* ***MUST*** have been produced no more than 12 months prior to the date it is provided to the DTA and ***MUST*** cover the latest *Major Production Release* of the *Applicant's Identity System* (if any) at the time of the *Accredited Provider's Annual Assessment*.

2.4 Functional Assessment and Usability Testing Requirements

TDIF Req: ANNUAL-02-04-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* must ensure an *Assessor* conducts the following Functional Assessments by the anniversary of the *Accredited Provider's* accreditation date each year:

a) a Privacy Assessment in accordance with ANNUAL-02-09-05
b) a Security Assessment in accordance with ANNUAL-02-09-06
c) a Penetration Test in accordance with ANNUAL-02-09-07; and
d) an Accessibility Assessment in accordance with ANNUAL-02-09-08.

TDIF Req ANNUAL-02-04-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
Subject to ANNUAL-02-04-02a, the *Accredited Provider* ***MUST*** ensure a user researcher conducts a Usability Test in accordance with ANNUAL-02-09-09 by the anniversary of the *Accredited Provider's* accreditation date each year.

TDIF Req: ANNUAL-02-04-02a; **Updated**: Mar-22; **Applicability**: A, C, I, X
ANNUAL-02-04-02 does not apply if the *Accredited Provider* has demonstrated to the DTA that the *Accredited Provider has* no interaction with a user when providing the services for which the *Accredited Provider* is accredited for.

TDIF Req: ANNUAL-02-04-02b; **Updated**: Mar-22; **Applicability**: A, C, I, X
ANNUAL-02-04-02 does not apply if the *Accredited Provider* has demonstrated to the DTA that the *Accredited Provider:*

1. either:
    a) has limited interaction with a *User* when providing the services for which the *Applicant* is accredited, including where the *User* is interacting with the *Accredited Provider*'s *Identity System;* or

b) has assessed and can demonstrate that there have been no relevant changes to the *Accredited Provider*'s *Identity System* in the 12 months prior to the date of the annual assessment; and

2. has determined, through a risk assessment, that there is a low risk that the failure to conduct the usability testing will adversely impact the usability of the *Accredited Provider*'s *Identity System*; and
3. the *Accredited Provider* has taken reasonable steps, including processes and procedures, to:
    a) obtain and record feedback from *Users* about the usability of the *Accredited Provider*'s *Identity System*; and
    b) incorporate such feedback into the design of its *Identity System*.

2.5 Skills, experience and independence of Assessors and User Researcher

TDIF Req: ANNUAL-02-05-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* MUST demonstrate to the *DTA* how each *Assessor* and User Researcher has relevant, reasonable and adequate experience, training and qualifications to conduct the relevant *Functional Assessment*.

TDIF Req: ANNUAL-02-05-01a; **Updated**: Jun-21; **Applicability**: A, C, I, X
The *Accredited Provider* MUST demonstrate to the *DTA* how the *Assessors*[4]:

a) Are independent from the development and operational teams of the *Accredited Provider's Identity System*.
b) Do not possess a conflict of interest in performing the *Functional Assessment* on the *Accredited Provider's Identity System*

[4] The requirements of ANNUAL-02-03-01a do not apply to user researchers conducting usability testing.

2.6 Annual Assessment schedule

TDIF Req: ANNUAL-02-06-01; **Updated**: Jun-21; **Applicability**: A, C, I, X }
Annual Assessments that occur during:

a) Even calendar years (i.e. 2022, 2024, 2026 etc) require that *Functional Assessments* *MUST* be undertaken by *Assessors* who are external to the *Accredited Provider's* organisation.
b) Odd calendar years (i.e. 2023, 2025, etc) *MAY* be undertaken by *Assessors* who are external to the development and operational teams of the *Accredited Provider's Identity System.*

2.7 Functional Assessment process

TDIF Req: ANNUAL-02-07-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* *MUST* ensure *Assessors* and the *User Researcher(s)* have access to and consider all relevant evidence provided by the *Accredited Provider* to the *DTA*. This includes any responses by the *DTA* to questions which may have been asked.

TDIF Req: ANNUAL-02-07-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
As part of the *Functional Assessments*, the *Assessors* *MUST* undertake the following activities:

a) Documentation reviews.
b) Interviews with key *Personnel*.
c) A run through of the *Accredited Provider's Identity System*.

TDIF Req: ANNUAL-02-07-03; **Updated**: Jun-21; **Applicability**: A, C, I, X
If required by an *Assessor* or the *DTA*, the *Accredited Provider* *MUST* take reasonable steps to permit the *Assessor* to undertake a site visit to the *Accredited Provider's* premises or other location where it provides services in connection with its *Identity System*.

TDIF Req: ANNUAL-02-07-04; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* *MUST* ensure that each *Assessor* prepares a report on the outcomes of the relevant *Functional Assessment* that includes:

a) test results where applicable
b) an assessment of whether the *Accredited Provider's Identity System* meets the applicable requirements of the TDIF
c) recommendations by the *Assessor*; and
d) such other information required by the *Accredited Provider* to enable the *Accredited Provider* to comply with the TDIF and prepare the *Annual Assessment Report*.

2.8 Annual Assessment Reports

TDIF Req: ANNUAL-02-08-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* ***MUST*** document the outcomes of each *Functional Assessment* in an *Annual Assessment Report,* which ***MUST*** include the following:

a) A summary of the activities performed by the *Assessor* during the *Functional Assessment*
b) The dates on which the *Functional Assessments* were commenced and completed
c) Name, role (or position) and contact details of the relevant *Accountable Executive* and point of contact
d) Qualifications and basis of independence for all *Assessors* used
e) Names and version numbers of all documents used by the *Accredited Provider*
f) City, state and (if applicable) country of all physical locations used in the *Accredited Provider'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 Provider's* operations are performed
g) The test or evaluation methodology(s) used
h) The test or evaluation results and findings
i) The opinion of the *Assessor* or user researcher (as applicable) on whether the *Accredited Provider's Identity Facility* meets the applicable *TDIF* requirements, including any requirements that could not be adequately assessed due to access or timing issues

j) Details of any identified instance of non-compliance with the TDIF requirements or any other risk identified by the *Assessor* or user researcher; and
k) Any recommendation from the *Assessor* or user researcher to address such non-compliance or risk.

2.8.1 *Forward Work Plan*

A *Forward Work Plan* is only applicable to risks, recommendations and non-compliances identified by an *Assessor* as part of a *Functional Assessment*.

TDIF Req: ANNUAL-02-08-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* *MUST:*

a) assess each identified instance of non-compliance with the TDIF requirements covered by the Annual Assessment reports submitted as per ANNUAL-02-08-01
b) Assess any other risks identified by the Assessor
c) Assign each instance of non-compliance and risk with a risk rating as set out in **Appendix A: Risk Ratings**; and
d) Include in the *Annual Assessment Report*:
    i. Details of each such risk assessment
    ii. A copy of the *Accredited Provider's* risk matrix; and
    iii. Descriptions of the likelihood and risk categories associated with the risk ratings assigned above.

TDIF Req: ANNUAL-02-08-02a; **Updated:** Mar-22; **Applicability:** A, C, I, X
The *Accredited Provider's Accountable Executive* *MUST* respond in writing to each recommendation, risk and non-compliance outlined in the *Annual Assessment Reports* including:

a) for each recommendation, risk and non-compliance that is accepted by the *Accredited Provider*, the timeframe and details of the actions that the *Accredited Provider* will take for implementation[5]; and

[5] This forms the basis for the Accredited Provider's Forward Work Plan

b) for each recommendation, risk and non-compliance that is not accepted by the *Accredited Provider*, the reasons for non-acceptance and details of alternative actions (if any) to be taken by the *Accredited Provider*.

TDIF Req: ANNUAL-02-08-03; **Updated**: Mar-22; **Applicability**: A, C, I, X

If the *Accredited Provider* does not implement a mitigation or recommendation by the timeframe set out in ANNUAL-02-08-02a, then its *Accountable Executive* *MUST* provide to the DTA in writing:

a) A revaluation of the risk
b) Any agreed upon mitigation strategies implemented, or being implemented, to manage the risk
c) Confirmation of the Applicant's tolerance to continue to carry the risk until the fix is implemented; and
d) The proposed new date for implementation that will be agreed upon by the DTA

NOTE: if the *Accredited Provider* has failed to implement a mitigation or recommendation following its written commitment as per ANNUAL-02-08-03, the DTA will then assess whether the *Accredited Provider* has failed to meet one or more of their ongoing obligations. If the DTA finds that the *Accredited Provider* has failed to meet their obligations, this will result in a finding of non-compliance with the TDIF, the DTA will make a decision whether the *Accredited Provider*'s accreditation will be suspended or *terminate*d.

TDIF Req: ANNUAL-02-08-04; **Updated**: Mar-22; **Applicability**: A, C, I, X

Any risks or recommendations identified in ANNUAL-02-08-02 or ANNUAL-02-08-03 *MUST NOT:*

- meet or exceed a High or Extreme risk rating[6] for the *Accredited Provider*'s Annual Assessment.

TDIF Req: ANNUAL-02-08-04a; **Updated**: Mar-22; **Applicability**: A, C, I, X

If the risk rating meets or exceeds that outlined above in ANNUAL-02-08-04, the *Accredited Provider* *MUST* confirm:

a) it has implemented mitigations to address the recommendation, risk or non-compliance

[6] According to Appendix A: Risk Ratings in TDIF 07 Maintain Accreditation, or the Applicant's equivalent risk framework.

b) The risk, recommendation or non-compliance has been reassessed and the residual risk rating is at Moderate or below[7]; and
c) The *Accountable Executive* has signed off and confirmed the implemented mitigation of the risk and the new residual risk rating.

High or Extreme Risks

According to **Appendix A: Risk Ratings**, *Accredited Providers* must be aware that a High risk rating is grounds for a failed Annual Assessment and that the DTA may suspend an *Accredited Provider*'s accreditation until the items required in ANNUAL-02-08-04a are complete and the DTA is satisfied that the risk is sufficiently mitigated.

According to **Appendix A: Risk Ratings**, *Accredited Provider*s must be aware that an Extreme risk rating is considered grounds for a failed Annual Assessment and immediate suspension of accreditation.

2.9 TDIF 04 Functional Requirements Review

TDIF Req: ANNUAL-02-09-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
As part of the *Annual Assessment* the *Accredited Provider* *MUST* review following FRAUD requirements in *TDIF 04 Functional Requirements* and provide the *DTA* with:

a) The annual assessment of the *Digital Identity Fraud Risk* associated with the services for which the *Accredited Provider* is accredited and the *Accredited Provider's Identity System* as per FRAUD-02-01-02
b) Where exceptional circumstances prevented or affected the *Applicant's* capability to implement a *TDIF* requirement, the record of decisions taken by the *Applicant* in relation to such non-compliance and remedial action as per FRAUD-02-01-04
c) Any decisions and supporting documentation made by the *Accredited Provider* to vary its fraud control arrangements during the year (as per FRAUD-02-01-04).
d) Evidence the *Accredited Provider* has reviewed its *Fraud Control Plan* (and supporting *Fraud Control Plans*) during the year (as per FRAUD-02-02-02 and FRAUD-02-02-02a).

[7] According to Appendix A: Risk Ratings in TDIF 07 Maintain Accreditation, or the Applicant's equivalent risk framework.

e) A copy of fraud awareness training materials provided by the *Accredited Provider* to *Personnel* during the year (as per FRAUD-02-03-01 and FRAUD-02-03-02).

TDIF Req: ANNUAL-02-09-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
As part of the *Annual Assessment* the *Accredited Provider* ***MUST*** review the following PRIV requirements in *TDIF 04 Functional Requirement*s and provide the *DTA* with:

a) Evidence the *Accredited Provider* has reviewed its *Privacy Policy* and where relevant updated during the year (as per PRIV-03-02-05).
b) Evidence the *Accredited Provider* has reviewed its *Privacy Management Plan* and where relevant updated during the year (as per PRIV-03-02-07).
c) A copy of privacy awareness training materials provided by the *Accredited Provider* to *Personnel* during the year (as per PRIV-03-02-08).
d) A copy of any Privacy Impact Assessments conducted on all *High Risk Projects* related to its *Identity System* (as per PRIV-03-03-01)

TDIF Req: ANNUAL-02-09-03; **Updated**: Mar-22; **Applicability**: X
As part of the *Annual Assessment* the *Accredited Provider* ***MUST*** provide the DTA with a copy of their *Annual Transparency Report* (as per PRIV-03-06-05 and PRIV-03-06-05a).

TDIF Req: ANNUAL-02-09-04; **Updated**: Mar-22; **Applicability**: A, C, I, X
As part of the *Annual Assessment* the *Accredited Provider* ***MUST*** review the following PROT requirements in *TDIF 04 Functional Requirements* and provide the *DTA* with:

a) The annual assessment of the *Cyber Security Risk* associated with the services for which the *Accredited Provider* is accredited and the *Accredited Provider's Identity System* as per PROT-04-01-01
b) Where exceptional circumstances prevented or affected the *Applicant's* capability to implement a *TDIF* requirement, the record of decisions taken by the *Applicant* in relation to such non-compliance and remedial action as per PROT-04-01-03
c) Any decisions and supporting documentation made by the *Accredited Provider* to vary its protective security arrangements during the year as per PROT-04-01-03

d) A copy of protective security training materials and evidence that training was provided by the *Accredited Provider* to *Personnel* during the year as per PROT-04-01-05a
e) Evidence the *Accredited Provider* has reviewed its *System Security Plan* (and supporting *System Security Plans*) and where relevant updated them during the year as per PROT-04-01-12 and PROT-04-01-13
f) Evidence the *Accredited Provider* has tested its *Disaster Recovery and Business Continuity Plan* during the year as per PROT-04-02-25.

2.9.1 Annual privacy assessment

TDIF Req: ANNUAL-02-09-05; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* ***MUST*** commission an *Assessor* to conduct a privacy assessment which ***MUST***, at a minimum:

a) include an assessment of whether the *Accredited Provider* has addressed all recommendations included in the privacy impact assessment prepared under ASSESS-07-05-01
b) address the recommendations (if any) included in a privacy impact assessment conducted by the *Accredited Provider* under PRIV-03-03-01 after the date of accreditation or the date of the last *Annual Assessment*
c) address the recommendations (if any) made by the Information Commissioner or a State or Territory privacy authority (as applicable), in respect of any complaints against the *Accredited Provider* or in respect of any privacy incidents involving the *Accredited Provider*; and
d) includes a review and assessment of the *Applicant's* compliance with the privacy requirements of the TDIF

2.9.2 Annual security assessment

TDIF Req: ANNUAL-02-09-06; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* ***MUST*** commission an *Assessor* to conduct a security assessment which ***MUST***, at a minimum:

a) address the findings and recommendations (if any) from the penetration testing of the *Accredited Provider's Identity System* conducted under ANNUAL-02-09-07

b) if the *Accredited Provider* has conducted penetration testing of a major production release of software forming part of its *Identity System* after the date of accreditation or the date of the last *Annual Assessment*—address the findings and recommendations (if any) from such testing
c) include an evaluation of the impact of the following events against the *Accredited Provider's* protective security controls:
   i. changes to the *Accredited Provider's* tolerance of *Cyber Security Risks*
   ii. *Cyber Security Incidents* reported to the DTA, and the *Accredited Provider's* response to such incidents; and
   iii. changes to the design of the *Accredited Provider's Identity System*
d) include an evaluation of the sufficiency of the *Accredited Provider*'s protective security controls
e) include a review and assessment of any decisions, together with supporting information, taken by the *Accredited Provider*'s CSO under PROT-04-01-03 to vary the *Accredited Provider's* protective security arrangements; and
f) include a review and assessment of the entity's compliance with the applicable requirements section 4 (Protective Security Requirements) of *TDIF: 04 Functional Requirements.*

2.9.3 Annual penetration test

TDIF Req: ANNUAL-02-09-07; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* MUST commission an *Assessor* to conduct penetration testing of its *Identity System* which must, at a minimum, meet the requirements of ASSESS-07-06-02.

2.9.4 Annual accessibility assessment

TDIF Req: ANNUAL-02-09-08; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* MUST commission an *Assessor* to conduct an accessibility assessment which must, at a minimum, assess whether the *Accredited Provider's Identity System* meets:

a) *WCAG* version 2.0 to the AA standard for web-based *Identity Systems*; and
b) *WCAG* version 2.1 to the AA standard for mobile-based *Identity Systems*.

2.9.5 Annual usability test

TDIF Req: ANNUAL-02-09-09; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Accredited Provider* ***MUST*** commission a user researcher to conduct a usability test which must, at a minimum, meet the requirements of UX-05-04-02 to UX-05-04-06b.

2.10 TDIF 05 Role Requirements Review

TDIF Req: ANNUAL-02-10-01; **Updated**: Mar-22; **Applicability**: I
If an *Identity Service Provider* supports *Exceptional Use Cases* as per IDP-03-03-01, it ***MUST*** review its processes and risk assessments as per IDP-03-03-01b and provide evidence of this review and any updated documentation to the DTA.

2.10.1 IDP Biometric Requirements

TDIF Req: ANNUAL-02-10-02; **Updated**: Mar-22; **Applicability**: I,
If an *Accredited Provider* operates biometrics in accordance with Section 3.8 of TDIF 05 Role Requirements, then it ***MUST*** implement the following requirements as part of its Annual Assessment and submit evidence of this review to the DTA.

TDIF Req: ANNUAL-02-10-03; **Updated**: Mar-22; **Applicability**: I,
The *Applicant* ***MUST*** consider the following risks related to performing *Biometric Binding* when reviewing their *Fraud Control Plan* and *System Security Plan* as part of its Annual Assessment requirements:

a) Applicable risks in IDP-03-08-03
b) Any *Major Production Releases* that impact the operation, or result in a substantive change to the performance, of the *Applicant's Biometric Capability*
    - The Applicant ***MUST*** provide a copy of their product release version documentation, including release notes, to the DTA
c) Changes in the biometric vulnerability landscape that impact the Applicant's operation of their *Biometric Capability*.
d) Risks related to identified attacks on the *Biometric Capability* that have occurred since the last assessment

NOTE: **biometric vulnerability landscape** refers to accessible and widespread emerging technology that may overcome a previously difficult way of fooling a PAD system or matching algorithm. For example, convincing silicon masks become much cheaper to acquire in a short period of time. Or in the case of 3d printers, widespread, cheaper access to the technology means there are more ways for more people to create attack artefacts.

TDIF Req: ANNUAL-02-10-03a; **Updated**: Mar-22; **Applicability**: I,
Evidence of the review and risks outlined in ANNUAL-02-10-03, associated mitigation strategies and treatments, the Applicant's risk framework and any supporting evidence *MUST* be provided to the DTA as part of the Annual Assessment.

TDIF Req: ANNUAL-02-10-03b; **Updated**: Mar-22; **Applicability**: I,
If the risk assessment undertaken by the Applicant in ANNUAL-02-10-03 indicates that substantial changes have occurred to the PAD technology of the *Accredited Provider*'s Biometric Capability, the PAD technology *MUST* be re-tested as per IDP-03-08-12 to IDP-03-08-12i and the report and any additional required evidence submitted to the DTA for review as part of the Annual Assessment.

TDIF Req: ANNUAL-02-10-03c; **Updated**: Mar-22; **Applicability**: I,
If the risk assessment undertaken by the Applicant in ANNUAL-02-10-03 indicates that substantial changes have occurred to the matching algorithm of the *Accredited Provider's Biometric Capability*, the Matching Algorithm *MUST* be re-tested as per IDP-03-08-18 to IDP-03-08-18d and the report and any additional evidence submitted to the DTA for review as part of the Annual Assessment.

TDIF Req: ANNUAL-02-10-04; **Updated**: Mar-22; **Applicability**: I,

If the *Accredited Provider* supports *Local Biometric Binding*, then it *MUST* review and record any variations to the locations used for *Local Biometric Binding* during the last 12 months as per IDP-03-08-14c and FRAUD-02-01-04.

TDIF Req: ANNUAL-02-10-05; **Updated**: Mar-22; **Applicability**: I,
If the *Accredited Provider* supports *Manual Face Comparison*, it *MUST* review and submit to the DTA evidence of:

a) The tools and annual training for *Personnel* performing identity proofing processes to detect fraudulent attributes and *Evidence of Identity Documents*[8]
b) *Assessing Officer* annual training and training material as per IDP-03-08-24
c) The *Assessing Officer* reference card as per IDP-03-08-24a
d) Its *Fraud Control Plan* and procedures to detect fraudulent activities by *Assessing Officers* performing *Manual Face Comparison* as per IDP-03-08-25 and FRAUD-02-02-01a
e) The quality control and quality assurance procedures for *Manual Face Comparison* decisions made by *Assessing Officers* and the *Accredited Provider*'s response to any risks that have arisen during operations as per IDP-03-08-26

2.10.2 ASP Annual Requirements

TDIF Req: ANNUAL-02-10-06; **Updated**: Mar-22; **Applicability**: A
As part of the *Annual Assessment* the *Accredited Provider* ***MUST*** provide the DTA with evidence of its arrangements with an *Authoritative Source* (as per ASP-05-02-01a)

2.11 Exemption Requests Review

As the justification for exemptions may change, and the risk environment will continue to evolve over time, it is important that *Accredited Providers* update their approval for exemptions as part of their *Annual Assessments*. This allows the *DTA* to review the exemption and either continue to approve or, if necessary, reject it if the justification or residual risk is no longer acceptable. The DTA's delegate will assess the information provided and in accordance with the Exemption Process set out in Appendix A of *TDIF 03 Accreditation Process.*

TDIF Req: ANNUAL-02-11-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
If an *Accredited Provider* has been granted an exemption request as per ACCRED-03-01-06 and ACCRED-03-01-06a, then it ***MUST*** review the exemption request and:

a) Confirm that the Exemption Request is still required

[8] As per the requirements in Table 1: Identity Proofing Levels of TDIF 05 Role Requirements.

b) Reassess the risk and mitigation measures in place, including any new risks arising throughout the year in response to the *Accredited Provider*'s operations
c) Include a new date of expiry or review of the Exemption Request that is not more than 12 months from the date of the review
d) Have the *Accredited Provider*'s Accountable Executive confirm and sign off on the items above; and
e) Submit evidence of the above to the DTA.

The DTA's delegate will assess the Exemption Request according to the Exemption Process as set out in *Appendix A of TDIF 03 Accreditation Process* and decide if the *Accredited Provider*'s reasons for seeking the Exemption Request still meet the TDIF's objectives and guiding principles for accreditation.

Appendix A: Risk Ratings

Refer to the ISO 31000 or the *Accredited Provider's* own risk management framework for a description of likelihood and consequence ratings.

Extreme Risk. The *Accredited Provider* fails to meet a *TDIF* requirement, or an Assessor has identified a risk or recommendation, which results in extreme unmitigated risk.

- An extreme risk *MUST* result in a failed *Annual Assessment* as per ANNUAL-02-01-02a and ANNUAL-02-08-04.
- The DTA's delegate will consider immediate Suspension of an *Accredited Provider*'s accreditation, which may occur until such time as the extreme risk is sufficiently mitigated
- The DTA's delegate will consider whether a reaccreditation activity is required for the *Accredited Provider*'s *Identity System* once it has confirmed that the extreme risk is sufficiently mitigated as per ANNUAL-02-01-02b and ANNUAL-02-08-04a.
- If the *Accredited Provider* fails to mitigate the risk or rectify the TDIF non-compliance within the agreed timeframe, then the DTA may terminate the *Accredited Provider*'s accreditation.

High Risk. The *Accredited Provider* fails to meet a *TDIF* requirement, or an *Assessor* has identified a risk or recommendation, which results in high unmitigated risk.

- A high risk MUST result in a failed *Annual Assessment* as per ANNUAL-02-01-02a and ANNUAL-02-08-04.
- The DTA's delegate *MUST* consider immediate Suspension of an *Accredited Provider*'s accreditation, which may occur until such time as the high risk is sufficiently mitigated
- The DTA's delegate *MUST* consider whether a reaccreditation activity is required for the *Accredited Provider's Identity System* once it has confirmed that the high risk is sufficiently mitigated as per ANNUAL-02-01-02b and ANNUAL-02-08-04a.
- If the *Accredited Provider* fails to mitigate the risk or rectify the TDIF non-compliance within the agreed timeframe, then the DTA may *terminate* the *Accredited Provider*'s accreditation.

Moderate Risk. The *Accredited Provider* fails to meet a *TDIF* requirement, or an *Assessor* has identified a risk or recommendation which may result in moderate unmitigated risk.

- If the *Accredited Provider* fails to mitigate the risk or rectify the TDIF non-compliance within the agreed timeframe, then the DTA may suspend or *terminate* the *Accredited Provider*'s accreditation

Low Risk. The *Accredited Provider* fails to meet a *TDIF* requirement, or an *Assessor* has identified a risk or recommendation which may result in low unmitigated risk.

- If the *Accredited Provider* fails to mitigate the risk or rectify the TDIF non-compliance within the agreed timeframe, then the DTA may suspend or *terminate* the *Accredited Provider*'s accreditation

Compliant. The *Accredited Provider* has demonstrated with evidence they comply with a *TDIF* requirement or the intent of a requirement and there are no outstanding risks or recommendations associated with the requirement.

Not Applicable (N/A). A TDIF requirement that does not apply to an *Accredited Provider* as their *Identity System* does not use, rely on or support the *TDIF* requirement. The DTA will confirm non-applicability of requirements with the *Accredited Provider*.

.

Appendix B: Supporting documentation and information

Table 1: Accreditation Evidence

Document	Related **TDIF Req**uirement	Annual Requirement	**Applicability**	**Evidence Required**
TDIF 07 Maintain Accreditation		ANNUAL-02-01-01	A, C, I, X	DTA requested evidence - DTA to Advise if required
TDIF 07 Maintain Accreditation		ANNUAL-02-01-01a	A, C, I, X	Evidence to meet any new or amended requirements – DTA to advise if required
TDIF 07 Maintain Accreditation		ANNUAL-02-01-03	A, C, I, X	Changes to an Accredited Provider's Identity System – if applicable
TDIF 07 Maintain Accreditation		ANNUAL-02-02-01	A, C, I, X	Review TDIF Agreement (MOU)
TDIF 07 Maintain Accreditation		ANNUAL-02-02-04	A, C, I, X	Qualifying Attestation Letter
TDIF 03 Accreditation Process	ACCRED-03-01-06a	ANNUAL-02-11-01	A, C, I, X	Exemption Request Form and Evidence
TDIF 07 Maintain Accreditation	Section 7 Functional Assessments – TDIF 04 Functional Requirements	ANNUAL-02-04-01	A, C, I, X	Assessors must conduct e) a Privacy Assessment in accordance with ANNUAL-02-09-05 f) a Security Assessment in accordance with ANNUAL-02-09-06 g) a Penetration Test in accordance with ANNUAL-02-09-07; and h) an Accessibility Assessment in accordance with ANNUAL-02-09-08.
TDIF 07 Maintain Accreditation	UX-05-04-02 to UX-05-04-06b.	ANNUAL-02-04-02 ANNUAL-02-09-09	A, C, I, X	Usability Testing

TDIF 07 Maintain Accreditation		ANNUAL-02-04-02a ANNUAL-02-04-02b	A, C, I, X	Limited exemption evidence to usability testing required – if applicable
TDIF 07 Maintain Accreditation	Section 7 Functional Assessments – TDIF 04 Functional Requirements	ANNUAL-02-08-01	A, C, I, X	Functional Assessment Reports (for each functional assessment conducted under ANNUAL-02-04-01 and relevant other requirement numbers)
TDIF 07 Maintain Accreditation		ANNUAL-02-08-02 ANNUAL-02-08-02a	A, C, I, X	Accountable Executive response to risks, recommendations and non-compliances identified by an Assessor as part of a Functional Assessment – if applicable
TDIF 07 Maintain Accreditation		ANNUAL-02-08-03	A, C, I, X	Review of any outstanding items in the *Forward Work Plan* – if applicable
TDIF 07 Maintain Accreditation	FRAUD-02-01-02	ANNUAL-02-09-01	A, C, I, X	Assessment of the Digital Identity Fraud Risk (incorporated in Fraud Control Plan)
TDIF 07 Maintain Accreditation	FRAUD-02-01-04	ANNUAL-02-09-01	A, C, I, X	Where exceptional circumstances prevented or affected the *Applicant's* capability to implement a *TDIF* Fraud requirement, the record of decisions taken by the *Applicant* in relation to such non-compliance and remedial action
TDIF 07 Maintain Accreditation	FRAUD-02-01-04	ANNUAL-02-09-01		Any decisions and supporting documentation made by the *Accredited Provider* to vary its fraud control arrangements during the year
TDIF 07 Maintain Accreditation	FRAUD-02-02-02 FRAUD-02-02-02a	ANNUAL-02-09-01	A, C, I, X	Review Fraud Control Plan
TDIF 07 Maintain Accreditation	FRAUD-02-03-01 FRAUD-02-03-02	ANNUAL-02-09-01	A, C, I, X	Review fraud awareness training material
TDIF 07 Maintain Accreditation	PRIV-03-02-05	ANNUAL-02-09-02	A, C, I, X	Evidence of a review of the Privacy Policy

TDIF 07 Maintain Accreditation	PRIV-03-02-07	ANNUAL-02-09-02	A, C, I, X	Privacy Management Plan
TDIF 07 Maintain Accreditation	PRIV-03-02-08	ANNUAL-02-09-02	A, C, I, X	Privacy awareness training material
TDIF 07 Maintain Accreditation	PRIV-03-03-01	ANNUAL-02-09-02	A, C, I, X	A copy of any PIAs conducted on *High Risk Projects* related to the Accredited Provider's Identity System – if applicable
TDIF 07 Maintain Accreditation	PRIV-03-06-05 PRIV-03-06-05a	ANNUAL-02-09-03	X	Annual Transparency Report
TDIF 07 Maintain Accreditation	PROT-04-01-01	ANNUAL-02-09-04	A, C, I, X	Assessment of the Cyber Security Risks (incorporated in System Security Plan)
TDIF 07 Maintain Accreditation	PROT-04-01-03	ANNUAL-02-09-04	A, C, I, X	Where exceptional circumstances prevented or affected the *Applicant's* capability to implement a *TDIF* protective security requirement, the record of decisions taken by the *Applicant* in relation to such non-compliance and remedial action
TDIF 07 Maintain Accreditation	PROT-04-01-03	ANNUAL-02-09-04	A, C, I, X	Any decisions and supporting documentation made by the *Accredited Provider* to vary its protective security arrangements during the year
TDIF 07 Maintain Accreditation	PROT-04-01-05a	ANNUAL-02-09-04	A, C, I, X	Review Security awareness training material
TDIF 07 Maintain Accreditation	PROT-04-01-12 PROT-04-01-13	ANNUAL-02-09-04	A, C, I, X	Review System Security Plan
TDIF 07 Maintain Accreditation	PROT-04-02-25	ANNUAL-02-09-04	A, C, I, X	Evidence the Accredited provider has tested its Disaster Recovery and Business Continuity Plan (DRBCP)
TDIF 07 Maintain Accreditation	IDP-03-03-01b	ANNUAL-02-10-01	I	If applicable - review of processes and risk assessments relating to Exceptional Use Cases
TDIF 07 Maintain Accreditation	IDP-03-08-03	ANNUAL-02-10-03 ANNUAL-02-10-03a	I	Review Biometric Binding Fraud Risks (can be incorporated into Fraud Control Plan and System Security Plan)

TDIF 07 Maintain Accreditation	IDP-03-08-12 – IDP-03-08-12i	ANNUAL-02-10-03b	I	If required - Presentation Attack Detection (PAD) test Report
TDIF 07 Maintain Accreditation	IDP-03-08-18 - IDP-03-08-18d	ANNUAL-02-10-03c	I	If required - Technical Biometric Matching Algorithm test Report
TDIF 07 Maintain Accreditation	IDP-03-08-14c FRAUD-02-01-04	ANNUAL-02-10-04	I	If applicable - review and record any variations to the locations used for *Local Biometric Binding* during the last 12 months
TDIF 07 Maintain Accreditation	IDP-03-08-24 - IDP-03-08-24b	ANNUAL-02-10-05	I	*Assessing Officer Manual Face Comparison* training materials *Assessing Officer Manual Face Comparison* procedures to detect Fraudulent activities. Quality control and assurance measures for decisions made by *Assessing Officers*
TDIF 07 Maintain Accreditation	ASP-05-02-01a	ANNUAL-02-10-06	A	Review of evidence of the arrangement with an Authoritative Source

Templates are available from the TDIF documents website.

Appendix C: Variations in Accreditation Documentation

Table 3: Variations of Accreditation Evidence Review

Document	TDIF Req	Applicability	Evidence Required	Review Required?
TDIF 03 Accreditation Process	ACCRED-03-01-01	A, C, I, X	TDIF Application Letter and Statement of Claims	Yes
TDIF 03 Accreditation Process	ACCRED-03-01-01	A, C, I, X	*Identity System* Architecture documents	Yes
TDIF 03 Accreditation Process	ACCRED-03-04-01	A, C, I, X	Qualifying Attestation Letter	Yes
TDIF 03 Accreditation Process	ACCRED-03-04-02	A, C, I, X	TDIF Agreement (MOU)	DTA to Advise
TDIF 03 Accreditation Process	ACCRED-03-01-06a	A, C, I, X	Exemption Request Form and Evidence	DTA to advise
TDIF 04 Functional Requirements	FRAUD-02-01-02	A, C, I, X	Assessment of the Digital Identity Fraud Risk (incorporated in Fraud Control Plan)	Yes
TDIF 04 Functional Requirements	FRAUD-02-02-01 FRAUD-02-02-01a	A, C, I, X	Fraud Control Plan	Yes
TDIF 04 Functional Requirements	FRAUD-02-03-01 FRAUD-02-03-02	A, C, I, X	Fraud awareness training material	Yes
TDIF 04 Functional Requirements	PRIV-03-02-03	A, C, I, X	Privacy Policy	Yes
TDIF 04 Functional Requirements	PRIV-03-02-06	A, C, I, X	Privacy Management Plan	Yes
TDIF 04 Functional Requirements	PRIV-03-02-08	A, C, I, X	Privacy awareness training material	Yes
TDIF 04 Functional Requirements	PROT-04-01-01	A, C, I, X	Assessment of the Cyber Security Risks (incorporated in System Security Plan)	Yes
TDIF 04 Functional Requirements	PROT-04-01-05a PROT-04-01-08	A, C, I, X	Security awareness training material	Yes
TDIF 04 Functional Requirements	PROT-04-01-11 PROT-04-01-11a	A, C, I, X	System Security Plan	Yes
TDIF 04 Functional Requirements	PROT-04-01-15a	A, C, I, X	Security maturity monitoring	Yes

TDIF 04 Functional Requirements	PROT-04-02-09	A, C, I, X	Procedures setting out criteria for Cyber Security Incident investigation processes	Yes
TDIF 04 Functional Requirements	PROT-04-02-24	A, C, I, X	Disaster Recovery and Business Continuity Plan (DRBCP)	Yes
TDIF 04 Functional Requirements	PROT-04-02-27	A, C, I, X	Cryptographic Key Management Plan (CKMP)	Yes
TDIF 04 Functional Requirements	UX-05-01-05	A, C, I, X	Individual end-to-end journey map of the Applicant's *Identity System*	Yes
TDIF 04 Functional Requirements	UX-05-04-02 UX-05-04-06b	A, C, I, X	Usability Test Plan and Usability testing	Yes
TDIF 04 Functional Requirements	TEST-06-01-01 TEST-06-01-02 TEST-06-01-03	A, C, I, X	Technical Testing evidence • Requirements Traceability Matrix • Technical Test Report	Yes
TDIF 04 Functional Requirements	ASSESS-07-01-01	A, C, I, X	Assessors must conduct a) a Privacy Impact Assessment in accordance with ASSESS-07-05-01 b) a Privacy Assessment in accordance with ASSESS-07-05-03 c) a Penetration Test in accordance with ASSESS-07-06-02 d) a Security Assessment in accordance with ASSESS-07-06-01; and e) an Accessibility Assessment in accordance with ASSESS-07-07-01.	Yes
TDIF 04 Functional Requirements	ASSESS-07-04-01 ASSESS-07-04-02 ASSESS-07-04-03	A, C, I, X	Functional Assessment Reports (for each functional assessment conducted under ASSESS-07-01-01 and the relevant other requirement number)	Yes

TDIF 05 Role Requirements	ROLE-02-01-01 ROLE-02-01-01a	A, C, I, X	User terms	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-03	I	Biometric Binding Fraud Risks (can be incorporated into Fraud Control Plan and System Security Plan)	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-07	I	Biometric Testing Entity qualifications evidence	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-12 – IDP-03-08-12i	I	Presentation Attack Detection (PAD) test Report	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-18 - IDP-03-08-18d	I	Technical Biometric Matching Algorithm test Report	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-24 - IDP-03-08-24b	I	*Assessing Officer Manual Face Comparison* training materials	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-54 IDP-03-08-26	I	*Assessing Officer Manual Face Comparison* procedures to detect Fraudulent activities. Quality control and assurance measures for decisions made by *Assessing Officers*.	DTA to advise
TDIF 05 Role Requirements	CSP-04-03-03g	C	Presentation Attack Detection (PAD) test Report	DTA to advise
TDIF 05 Role Requirements	ASP-05-02-01a	A	Evidence of the arrangement with an Authoritative Source	DTA to advise

Templates are available from the TDIF documents website.