Australian Government
Digital Transformation Agency

Accreditation Process

Trusted Digital Identity Framework
March 2019, version 1.3

dta

Digital Transformation Agency

The Digital Transformation Agency has tried to make the information in this product as accurate as possible. However, it does not guarantee that the information is totally accurate or complete. Therefore, you should not solely rely on this information when making a commercial decision.

Licence

Use of the Coat of Arms

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

Conventions

TDIF documents refenced by this document are denoted in italics. For example, *TDIF: Overview and Glossary* is a reference to the TDIF document titled Overview and Glossary.

The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" if used in this document are to be interpreted as described in the current version of the *Trusted Digital Identity Framework: Overview and Glossary.*

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document or have questions or comments please email the Director, Digital Identity Policy at identity@dta.gov.au.

Document management

The TDIF Accreditation Authority has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of changes
0.1	May 2017	SJP	Initial version
0.2	Sept 2017	SJP	Changed the accreditation process from a serial process to one that supports parallel activities. Now also aligns with changes to the other TDIF documents.
0.3	Sept 2017	SJP	Minor updates to support the public consultation draft.
0.4	Jan 2018	SJP	Incorporated feedback from stakeholders and public consultation.
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority.
1.1	Oct 2018	GJF & SJP	Updated the initial accreditation process and included the annual compliance and re-accreditation processes.
1.2	Jan 2019	GJF & SJP	Incorporated feedback from stakeholders.
1.3	Mar 2019	SJP	Incorporated feedback from public consultation.

Contents

1 Introduction

Agencies and organisations that apply to be accredited under the TDIF undergo a series of rigorous evaluations across all aspects of their identity service operations.

This document defines the TDIF Accreditation Process, the accreditation roles and responsibilities and requirements to be met for an Applicant to achieve and maintain accreditation. This document requires Applicants to demonstrate their identity service is usable, privacy enhancing and is secure and resilient to cyber threats. The intent of these evaluations is to determine whether the Applicant's identity service meets the TDIF Guiding Principles[1] and whether it is suitable to join the identity federation. This document does not define maximum periods in which individual activities, or the accreditation process is likely to take as this is largely driven by the Applicant.

It is expected the Applicant understands the requirements, compliance obligations and likely costs associated with pursuing and maintaining accreditation before commencing the TDIF Accreditation Process. An Applicant should be able to achieve TDIF accreditation within 12 months of submitting their Accreditation Plan. Factors that impact on the time taken to complete an activity or achieve accreditation include:

- The Applicant’s understanding of the accreditation process and requirements.
- The nature and maturity of the identity service being accredited.
- The Applicant’s business needs, threat environment and risk appetite.
- The degree to which the identity service is straightforward and easy to use.
- The time taken by the Applicant to complete the required independent evaluations and address any non-compliance issues to the satisfaction of the TDIF Accreditation Authority.

Although an Applicant should have an operational identity service prior to undergoing accreditation, the TDIF Accreditation Process supports Applicants that develop and mature their identity service over the course of accreditation. Applicants with fully operate identity services who are familiar with the TDIF requirements are likely to complete the TDIF Accreditation Process much quicker than an Applicant who is either unfamiliar with the process or is still developing their identity service.

[1] See *TDIF: Overview and Glossary* for further information on the TDIF guiding principles

The intended audience for this document includes:

- Applicants and Accredited Providers.
- Assessors.
- Relying Parties.
- TDIF Accreditation Authority[2].

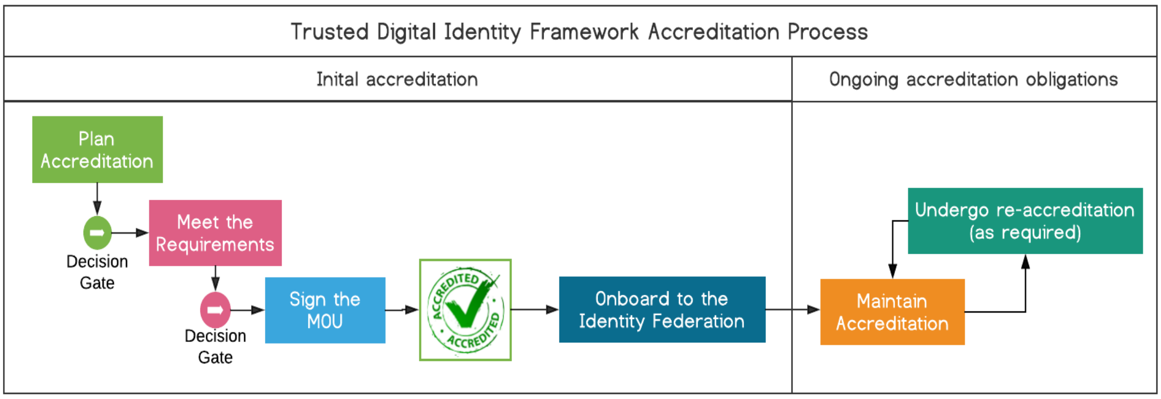
[2] The terms ‘TDIF Accreditation Authority’ and ‘TDIF Oversight Authority*’* are used interchangeably between TDIF documents and *TDIF: System Governance Interim Memorandum of Understanding*. Both terms refer to the same governance entity - Australian Government Chief Digital Officer, Digital Transformation Agency.

2 TDIF Accreditation Process

2.1 Overview

The TDIF Accreditation Process is a formal process through which Applicants demonstrate their ability to meet the initial and ongoing accreditation requirements to the satisfaction of the TDIF Accreditation Authority. Figure 1 below provides an overview of the TDIF Accreditation Process.

Figure 1: TDIF Accreditation Process.


Trusted Digital Identity Framework Accreditation Process
Inital accreditation
Ongoing accreditation obligations
Plan Accreditation
Decision Gate
Meet the Requirements
Decision Gate
Sign the MOU
ACCREDITED
Onboard to the Identity Federation
Maintain Accreditation
Undergo re-accreditation (as required)

Progress through the TDIF Accreditation Process is managed by a series of decision gates. The decision gates are used by the TDIF Accreditation Authority to evaluate the Applicant's progress towards accreditation and an Accredited Provider's ability to meet its ongoing accreditation obligations. Arrows show the relationships between accreditation activities and all activities can be iterated.

All costs associated with accreditation are to be met by the Applicant. Although the TDIF Accreditation Authority does not charge Applicants a fee to complete the accreditation process, it could cost the Applicant to complete certain accreditation criteria. For example, to pay for externally qualified independent assessors for the Privacy Impact Assessment (PIA) and Information Security Registered Assessors Program (IRAP). Depending on the complexity and timeliness of the evaluation to be performed, the cost to the Applicant could be more than expected. Applicants are encouraged to contact several Assessors to get a sense of the cost, duration and complexity of an assessment prior to engaging a particular Assessor.

Applicants can apply to undergo the TDIF Accreditation Process for at any stage in the development life cycle of their identity services, however, the TDIF Accreditation Authority will only grant accreditation to operational identity services. Accreditation will occur prior to an identity service being approved to onboard to the identity federation. The Accreditation Authority will not grant provisional or partial accreditations.

Once accredited, the Accredited Provider **MUST** demonstrate its ability maintain its accreditation. Each year the Accredited Provider **MUST** undertake an annual assessment which is to be completed by the anniversary of the date on which TDIF accreditation was initially granted.

Following accreditation, the Accredited Provider **MAY** be directed by the TDIF Accreditation Authority to undergo re-accreditation following a cyber security incident, or serious or repeated privacy breaches, or as a result of a changing threat or operating environment which materially impacts the identity service’s risk profile. If re-accreditation is required, it **MUST NOT** replace the annual assessment requirements.

3 TDIF accreditation roles and responsibilities

3.1 Applicant & Accredited Provider

The Applicant / Accredited Provider is responsible for:

- Formally advising the TDIF Accreditation Authority of its intention to undergo the TDIF Accreditation Process.
- Preparing all required documentation within agreed timeframes with the TDIF Accreditation Authority.
- Obtaining all relevant internal system accreditations and certifications from the appropriate authorities within the Applicant’s government agency or organisation throughout the TDIF Accreditation Process (i.e. as part of initial accreditation, annual assessments and re-accreditation).
- Obtaining the required independent assessments from Assessors.
- Provision of the relevant accreditation artefacts.
- Remediating all identified non-conformance and adverse findings to the satisfaction of the TDIF Accreditation Authority or its staff.
- Accepting the residual risk relating to their identity system. (For larger government agencies and organisations, residual risks may be accepted by their internal accreditation or certification authorities).
- Formally advising the TDIF Accreditation Authority of its intention to leave the program in the event it:
  - No longer wants to undergo the TDIF Accreditation Process.
  - Can no longer comply with TDIF requirements once accredited.
  - Chooses to no longer maintain its accreditation.

Upon completion of the TDIF Accreditation Process, the Applicant and the TDIF Accreditation Authority will sign the *TDIF: System Governance Interim Memorandum of Understanding* (MOU). This sets out the respective rights and obligations in relation to governance and administration of the TDIF identity federation for the provision of its identity services. This MOU also specifies arrangements in relation to:

- Accreditation and approval of Participants, including maintaining accreditation or approval.
- Dispute resolution.

- Termination, resignation and suspension of Participants.

Once accredited, the Accredited Provider **MUST:**

- Be able to demonstrate through an annual assessment that it continues to offer an identity service in a manner consistent with the documents and evaluations that formed the basis of its accreditation.
- Advise the TDIF Accreditation Authority of significant changes to their identity service, risk profile, environment or notice of breach (security or privacy).

3.2 TDIF Accreditation Authority

The TDIF Accreditation Authority and its staff are responsible for:

- Ensuring that the TDIF Accreditation Process is conducted with due care and in accordance with the published TDIF documents.
- Reviewing, within agreed timeframes, all relevant Applicant documentation to ensure conformance to the published TDIF documents.
- Considering all reports and recommendations from Assessors.
- Interpreting conformance against TDIF requirements.
- All decisions in relation to the accreditation of Applicants and ongoing accreditation of Accredited Providers, including decisions to accept a non-conformance against the TDIF requirements where it considers evidence provided by the Applicant is sufficient in favour of non-conformance.
- At its discretion and in consultation with Applicants and Accredited Providers, advise other federation members of its decision to grant or reject an exemption request.
- Formally accepting the residual risk of granting accreditation and subsequently onboarding the Accredited Provider’s system into the identity federation.

3.3 Assessors

Assessors are independent evaluators of business processes, documentation, systems and services who have the required skills, experience and qualifications to determine whether an Applicant has met specific requirements of the TDIF.

Assessors are responsible for:

- Assessing the Applicant's compliance against specific TDIF requirements.
- Documenting their findings, which:
    - Summarise the activities performed during the evaluation.
    - Report the Applicant's compliance against specific TDIF requirements
    - Suggest remediation actions to address areas of non-compliance or unmitigated risk.
    - Express an unmodified opinion[3] and recommend whether the Applicant has satisfied specific requirements of the TDIF or not.

Applicants <u>**MUST**</u> use Assessors for the following activities:

- PIA and privacy audit[4].
- IRAP and penetration test[5].
- User Experience testing[6].

[3] Refer to Australian Government Auditing and Assurance Standards Board ASA 700 with respect to opinions. Although this standard is focused on Financial Reporting the intent of the concepts in regard to opinions and communicating Key Audit Matters are to be applied.

[4] See *TDIF: Privacy Requirements* for further information.

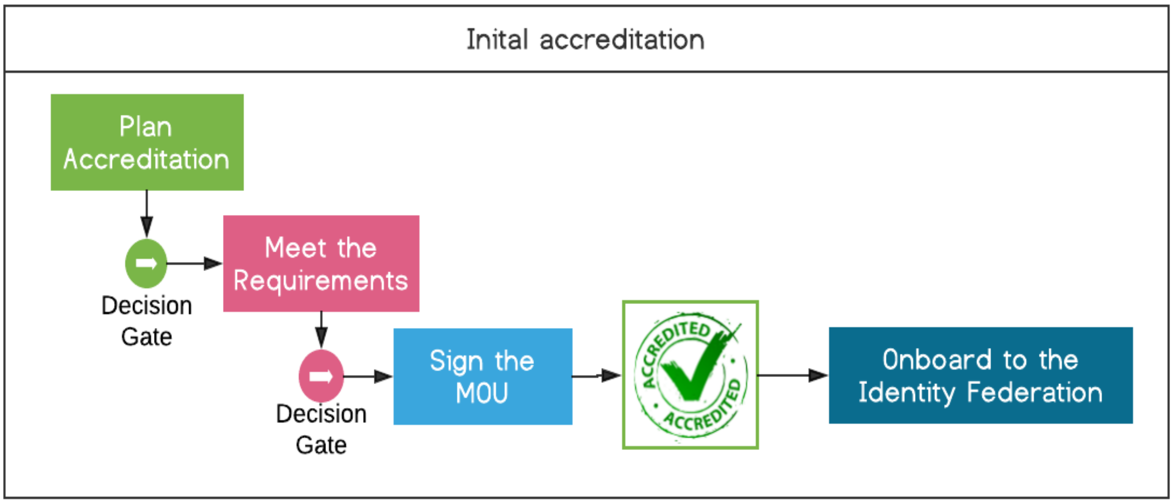
[5] See *TDIF: Protective Security Reviews* for further information.

[6] See *TDIF: User Experience Requirements* for further information.

4 Initial TDIF accreditation activities

TDIF accreditation requires the Applicant to adequately plan for and demonstrate its ability to meet foundation and relevant supplementary TDIF requirements. The initial TDIF accreditation process involves a combination of documentation, independent evaluations and operational testing. Successful completion of the process will result in the Applicant signing the TDIF MOU, being recognised as an Accredited Provider and being deemed suitable to onboard their service to the identity federation. The figure below outlines the initial TDIF accreditation process.

Figure 2: Initial TDIF accreditation process.



4.1 Plan Accreditation

The Applicant **MUST**:

- Formally advise the TDIF Accreditation Authority of its intention to undergo the TDIF Accreditation Process by submitting a TDIF Application Letter[7].
- Specify the accreditation service being sought:
    - Identity Service Provider.
    - Credential Service Provider.
    - Attribute Provider.
    - Identity Exchange.
    - Or any combination of the above.

[7] See Appendix A for the TDIF Application Letter template.

- Specify the assurance levels to be supported by their identity service:
  - For Identity Service Providers this means the Identity Proofing Levels.
  - For Credential Service Providers this means the Credential Levels.
- Provide a 'Statement of Applicability' which outlines which controls listed in the *TDIF: Protective Security Requirements* and *TDIF: Risk Management Requirements* will be implemented and for those that are applicable the way they will be implemented.
  - Any controls that will not be implemented **MUST** be covered by a TDIF exemption endorsed by an appropriate internal accreditation or certification authority within the Applicant's government agency or organisation[8].
- Provide the TDIF Accreditation Authority with all relevant exemptions against these controls.
  - The TDIF Accreditation Authority has the authority to either accept or reject the exemption for the purpose of TDIF accreditation. If the exemption is rejected the Applicant **MUST** implement the control as defined in the relevant TDIF document.
- Supply a completed Accreditation Plan to the TDIF Accreditation Authority, which outlines the approach to be taken by the Applicant to complete each accreditation activity.

The Accreditation Plan **MUST** set out as a minimum:

- The names, contact details and areas of responsibility of those responsible for the development of the Accreditation Plan.
- A description of how the Applicant will demonstrate it has satisfied each accreditation activity.
- A proposed workplan, with key dates, milestones and an indicative accreditation date listed.
- A description of how the Applicant will resolve adverse findings throughout initial accreditation.

The TDIF Accreditation Authority **MUST**:

- Ensure the applicable TDIF documents are available to the Applicant in a timely manner (see section titled '*Meet the Requirements'* for further details).

[8] See Appendix B for the TDIF exemption process.

- Formally acknowledge the Applicant’s intention to undergo accreditation in writing.
- Advise the Applicant of its decision to either accept or reject the Accreditation Plan and any exemptions received.

4.2 Plan accreditation decision gate

The TDIF Accreditation Authority **MUST** advise the Applicant whether the Accreditation Plan is sufficiently detailed to progress beyond the ‘*Plan Accreditation’* decision gate.

- If the Accreditation Plan is sufficiently detailed, the TDIF Accreditation Authority will advise the Applicant accordingly and will approve the Applicant to progress beyond the Governance decision gate.
- If the Accreditation Plan is not sufficiently detailed the TDIF Accreditation Authority will advise the Applicant accordingly, state the reasons why approval has not been granted and the required actions to be taken by the Applicant in order for them to be approved to move beyond the Governance decision gate.

4.3 Meet the requirements

The TDIF sets the minimum requirements that government agencies and organisations need to meet in order to achieve and maintain TDIF accreditation. This includes a set of foundation and supplementary requirements. Foundation requirements are applicable to all accreditation classes. Supplementary requirements apply for specific accreditation classes or in certain circumstances.

Foundation TDIF requirements:

- *TDIF: Privacy Requirements.*
- *TDIF: Protective Security Requirements.*
- *TDIF: Protective Security Reviews.*
- *TDIF: Risk Management Requirements.*
- *TDIF: Fraud Control Requirements.*
- *TDIF: User Experience Requirements.*
- *TDIF: Technical Requirements.*

- *TDIF: Attribute Profile.*
- *TDIF: OpenID Connect 1.0 Profile.*
- *TDIF: Technical Integration Testing Requirements.*
- *TDIF: Service Operations Requirements.*
- *TDIF: System Governance Interim Memorandum of Understanding.*

Supplementary TDIF requirements:

- *TDIF: Identity Proofing Requirements* – applicable when the service being accredited is an Identity Service Provider[9] [10].
- *TDIF: Authentication Credential Requirements* – applicable when the service being accredited is a Credential Service Provider.
- *TDIF: Attribute Provider Requirements* – applicable when the service being accredited is an Attribute Provider[11].
- *TDIF: SAML 2.0 Profile* – applicable if the Applicant's identity service supports SAML 2.0.

The Applicant **MUST**:

- Demonstrate its identity service conforms to the foundation TDIF requirements and all applicable supplementary TDIF requirements.
- Provide Assessor Findings reports for the PIA, privacy audit, IRAP, penetration test and user experience testing.
- Respond to any requests or questions raised by the TDIF Accreditation Authority or its staff in relation to the Applicant's conformance with TDIF requirements.
- Remediate any non-compliances or adverse findings to the satisfaction of the TDIF Accreditation Authority or its staff.

4.4 Meet the requirements decision gate

The TDIF Accreditation Authority **MUST**:

[9] Identity Service Providers **MUST** also meet the requirements listed in *Appendix E: Use of verified attributes outside the identity federation* of this document.

[10] Identity Service Providers **MUST** also meet the requirements listed in *Appendix F: Restricted Attributes* of this document.

[11] Attribute Providers **MUST** also meet the requirements listed in *Appendix E: Use of verified attributes outside the identity federation* of this document.

- Advise the Applicant of areas of compliance and non-compliance against the foundation TDIF requirements and applicable supplementary requirements.
- Advise the Applicant whether the proposed remediation actions are acceptable or not. If the proposed remediation actions are not acceptable, the TDIF Accreditation Authority or its staff will state the reasons why the actions are not accepted, and what the Applicant will need to do in order for its proposed remediation actions to be acceptable.

4.5 Sign the MOU

Upon successful completion of the '*Meet the Requirements'* activity, the Applicant's identity service will be recognised as meeting the TDIF initial accreditation requirements. The Applicant will be formally accredited against the TDIF.

The Applicant **MUST** sign two copies of the TDIF MOU and return both copies to the TDIF Accreditation Authority.

The TDIF Accreditation Authority **MUST** counter-sign two copies of the TDIF MOU and return one to the Applicant (who from this point on will be referred to as an Accredited Provider).

4.6 Onboard to the identity federation

Once accreditation has been granted, the Accredited Provider's system will be approved to onboard to the identity federation. A period of operation will follow, where rapid fixes may be required by the Accredited Provider to resolve issues or minor defects not discovered during the initial accreditation process.

During this period the Accredited Provider **MUST** provide reports for:

- Technical integration testing.
- Service operations readiness.

The TDIF Accreditation Authority **MUST**:

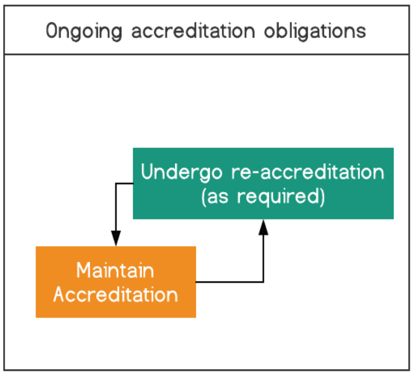
- Advise the Accredited Provider of areas of compliance and non-compliance against the technical integration testing and service operations requirements.

- Advise the Accredited Provider whether the proposed remediation actions are acceptable or not. If the proposed remediation actions are not acceptable, the TDIF Accreditation Authority or its staff will state the reasons why the actions are not accepted, and what the Accredited Provider will need to do in order for its proposed remediation actions to be acceptable.

5 Ongoing TDIF accreditation obligations

Once initial accreditation has been granted, the Accredited Provider is required to continually meet its TDIF obligations to the satisfaction of the TDIF Accreditation Authority and its staff. The figure below outlines these ongoing TDIF accreditation obligations.

Figure 3: Ongoing TDIF accreditation obligations.


Ongoing accreditation obligations
Undergo re-accreditation (as required)
Maintain Accreditation

5.1 Maintain accreditation

Once accredited, each Accredited Provider **MUST** continue to meet the obligations outlined in the TDIF MOU. This includes the requirement to undergo an annual assessment by the anniversary of their accreditation date and undergoing reaccreditation where directed.

5.1.1 Annual assessments

The purpose of the annual assessment is to determine whether the Accredited Provider continues to demonstrate its ability to meet TDIF requirements. It enables the Accredited Provider's internal certification authority, TDIF Accreditation Authority and identity federation participants to have confidence in the functionality and trustworthiness of the Accredited Provider's identity service.

To maintain accreditation each year the Accredited Provider **MUST** provide the TDIF Accreditation Authority with:

- An annual **Assessment Plan**, which describes the annual assessment activities to be undertaken, the people involved in undertaking these activities and any additional internal or external assessments planned for the identity service.

- An annual **Assessment Report** which details the Accredited Provider's annual compliance against the TDIF requirements and the implementation and effectiveness of the controls for the identity service.

- An annual **Qualifying Attestation Letter** signed by the Accredited Provider's relevant internal accreditation or certification authority which supports the claims made in the Assessment Report. The annual assessment **MUST** be undertaken by suitably qualified assessors and every second annual assessment **MUST** involve independent assessors who are external to the Accredited Provider's agency or organisation.

Every annual assessment that falls on an odd calendar year (e.g. 2019, 2021, 2023, etc) **MAY** be undertaken by internal staff independent from the operation and management of the identity service. Annual assessments that fall on even calendar years (e.g. 2020, 2022, 2024, etc) **MUST** be undertaken by independent assessors who are external to the Accredited Provider's government agency or organisation. Further information is provided in the section titled '*Annual Assessment Reports'*, below.

Unless otherwise agreed with the TDIF Accreditation Authority or its staff, the Accredited Provider **MUST** submit their Assessment Report, along with the accompanying Qualifying Attestation Letter, and the next year's Assessment Plan, prior to the anniversary of their initial accreditation. Upon receipt of the reports and attestation letter, the TDIF Accreditation Authority or its staff will conduct a review of them and advise the Accredited Provider of its acceptance or not, including whether the proposed remediation actions, and timings, are acceptable[12].

[12] If the proposed remediation actions are not acceptable, the TDIF Accreditation Authority or its staff will advise the Accredited Provider accordingly, state the reasons why the actions are not accepted, and what the Accredited Provider will need to do in order for its proposed remediation actions to be acceptable.

The Accredited Provider **MUST** remediate any non-compliances or adverse findings to the satisfaction of the TDIF Accreditation Authority or its staff within agreed timeframes.

To enhance trust and transparency in the identify federation the TDIF Accreditation Authority will publish the Qualifying Attestation Letter onto its public dashboard.

5.1.2 Annual Assessment Plan

The annual Assessment Plan **MUST:**

- Identify the period which is covered by the assessment, both internal and external assessment activities planned for the period and the proposed approach for each assessment activity.
- Document the process for objectively obtaining and evaluating evidence that will enable the TDIF Accreditation Authority to determine whether the Accredited Provider continues to meet the TDIF requirements.

When developing the annual Assessment Plan it is recommended it be informed by previous annual Assessment Reports and endorsed by the Accredited Provider's internal accreditation or certification authority as the outcomes of the annual assessment will provide input into the Accredited Provider's Annual Assessment Report.

5.1.3 Annual Assessment Report

The outcome of the annual assessment is an annual Assessment Report and a Qualifying Attestation Letter. The Assessment Report details the identity service's compliance against the TDIF requirements and the implementation and effectiveness of the measures for the system. This includes areas of compliance and non-compliance against the TDIF (documented in the Requirements Self-Assessment Report) and any suggested remediation actions. The Accredited Provider **MUST** use the compliance ratings listed in *Appendix D: Compliance ratings* when determining compliance or non-compliance.

The Accredited Provider **MUST** include the following reports as part of the annual Assessment Report:

- An annual Requirements Self-Assessment Report.
    - This may be undertaken by internal staff every calendar year.
- An annual Privacy Audit Report.
    - On odd calendar years this may be undertaken by internal staff.
    - On even calendar years this must be undertaken by an independent assessor.
- An annual Fraud Control Report.
    - This may be undertaken by internal staff every calendar year.
- An annual Business Continuity and Disaster Recovery Test Report.
    - This may be undertaken by internal staff every calendar year.
- An annual Vulnerability Assessment Report.
    - This may be undertaken by internal staff every calendar year.
- An annual Information Security Penetration Test Report.
    - On odd calendar years this may be undertaken by internal staff.
    - On even calendar years this must be undertaken by an independent assessor.
- An annual User Experience Report.
    - On odd calendar years this may be undertaken by internal staff.
    - On even calendar years this must be undertaken by an independent assessor.
- An annual Service Operations Report.
    - This may be undertaken by internal staff every calendar year.
- An annual Transparency Report[13] (if the Accredited Provider is an Identity Exchange).
    - This may be undertaken by internal staff every calendar year.

In addition to the above, every even calendar year the Accredited Provider **MUST** have an external IRAP Assessment[14] undertaken on their identity service by an independent assessor. The findings resulting from the IRAP Assessment **MUST** be included in the annual Assessment Report.

[13] Refer to *TDIF: Privacy Requirements* for further information.

[14] Refer to *TDIF: Protective Security Reviews* for further information.

The annual Assessment Report **SHOULD** include the following:

- The date of and period covered by the report.
- Name, role/position and contact details of the relevant internal accreditation or certification authority and point of contact within the Accredited Providers government agency or organisation.
- Qualifications and basis of independence for all Assessors utilised.
- Names and version numbers of all documents used by the Accredited Provider to disclose its business practices.
- City, state and (if applicable) country of all physical locations used in the Accredited Providers operations. This includes data centre locations (primary and alternate sites) and all other locations where general IT and business process controls that are relevant to the Accredited Providers operations are performed.
- Outcomes against the proposed annual Assessment Plan, including any lessons learnt.
- Express an opinion and assessed compliance of the Accredited Provider's identity service against the requirements of the TDIF.
- Provide a recommendation to the TDIF Accreditation Authority whether or not the Accredited Providers identity service continues to satisfy the TDIF requirements.
- Include a list of compliant and non-compliant controls.
- Where a non-compliance has been identified, the Report **MUST** recommend the remedial action to be undertaken by the Accredited Provider and the timeframe within which the actions are to be completed to address the non-compliance.

5.1.4 Qualifying Attestation Letter

The Qualifying Attestation Letter **MUST**, at a minimum, contain information that supports the Accredited Provider's claim that its operations are in accordance with TDIF MOU and TDIF requirements.

In addition, the Qualifying Attestation Letter **MUST** be signed by the Accredited Provider's relevant internal accreditation or certification authority and include the name, role/position and contact details of the authority that is asserting that the Accredited Provider’s identity service complies with TDIF requirements.

The Accredited Provider **SHOULD** publish the Qualifying Attestation Letter onto its public dashboard.

5.2 Undergo 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 service, other activities may necessitate a need for re-accreditation 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 or privacy).
- 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.

Other than meeting annual accreditation obligations, an Accredited Provider **MAY** be directed by the TDIF Accreditation Authority or its staff to undergo re-accreditation. This will occur if the Accredited Provider’s identity service is changed in a manner that may result in:

- Significant impacts to the Accredited Provider’s protective security arrangements.
- Serious or repeated privacy breaches (including of the TDIF Privacy Requirements or the Australian Privacy Principles).
- Material changes the Accredited Provider’s risk exposure.
- Material changes to the risk exposure of other participants in the identity federation that materially impact the Accredited Provider.

- After a significant change to the 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 a system, for example, a software vendor announces a critical vulnerability in a product used by the Applicant.

Re-accreditation **MAY** include IRAP assessments, penetration testing, vulnerability assessments or security risk assessments. In such circumstances, the TDIF Accreditation Authority or its staff will state the re-accreditation requirements to be met in writing. The costs associated with these activities **MUST** be met by the Accredited Provider and **MUST NOT** replace their annual compliance obligations.

To assist in the re-accreditation of identity services, Accredited Providers are encouraged to reuse as much information from previous accreditations as possible including, where appropriate, concentrating on the difference between the security posture of the identity service at the time of the last accreditation and the current security posture of the identity service.

5.2.1 Alternative assurance measures

Where authorised by the TDIF Accreditation Authority or its staff, an Accredited Provider **MAY** utilise alternate accreditation activities (e.g., PCI-DSS, ISO 27001, etc) where they can be shown to map to the TDIF requirements, including any additional TDIF requirements in the annual Assessment Report, and occur during the period being reported upon.

Where an Accredited Provider proposes to utilise an alternate assurance measure they **MUST** seek approval from the TDIF Accreditation Authority or its staff and provide a document that clearly maps the proposed measure against the TDIF requirements and for any TDIF requirement that does not directly map articulates how this will be achieved and reported. Once approval is obtained such an activity can be reflected in the annual Assessment Plan.

Appendix A : TDIF Application Letter template

[Applicant's letterhead]

[date]

Trusted Digital Identity Framework (TDIF) Accreditation Authority
Digital Transformation Agency
50 Marcus Clarke Street
Canberra, ACT 2600

Attention: Mr Peter Alexander.

Application for Trusted Digital Identity Framework accreditation

Dear Peter,

In accordance with the TDIF Accreditation Process, *[Applicant's name]* wishes to undergo accreditation as *[specify accreditation service: e.g. Identity Service Provider, Credential Service Provider, Attribute Provider, Identity Exchange, or a combination of these]* and provide *[this service / these services]* to the assurance level *of [Identity Proofing Level (IP) 1 – 4 for IdPs, Credential Level (CL) 1 – 3 for CSPs].*

[add a company profile, e.g. purpose/strengths/approach/value of Applicant's offerings. Also mention whether the Applicant is/is not Australian owned].

At this stage we expect to commence accreditation by *[date]* and anticipate completing all accreditation activities by *[date].* Attached is our Accreditation Plan which includes our proposed workplan. *[don't forget to include the Accreditation Plan]*

Also attached is our Statement of Applicability. *[don't forget to attach the Statement of Applicability and include any relevant exemptions]*

We look forward to working with you over the coming months on TDIF accreditation. I can be contacted on *[contact number]* and *[email].*

Yours sincerely,

[Name]

[Position]

[optional information: Applicant's corporate information and website]

Appendix B : TDIF exemption process

B.1 Purpose

This document outlines the TDIF exemption process to be used by Applicants and Accredited Providers (hereafter collectively referred to as 'Participants') when seeking an exemption against a TDIF requirement. This process can be used for any activity throughout the TDIF Accreditation Process, including initial accreditation or for TDIF obligations once accredited.

Any request for an exemption against a TDIF requirement **MUST**:

- Be signed off by the Participant's relevant internal certification or accreditation authority *before* it is submitted to the TDIF Accreditation Authority[15] for approval.
- Be supported by evidence which is provide to the TDIF Accreditation Authority as part of the exemption request.

B.2 General

The TDIF Accreditation Process defines the requirements to be met by government agencies and organisations in order to achieve and maintain TDIF accreditation for their identity service. The TDIF MOU, Part D, details the requirements related to the accreditation and approval of Participants.

During the TDIF Accreditation Process, the DTA needs to:

- Interpret the Applicants conformance, or non-compliance, against the TDIF Accreditation Criteria[16].
- Review and agree any proposed remediation actions.
- Review and agree any non-compliance submissions.
- Advise the Oversight Authority of the residual risk to the federation regarding the accreditation of the Applicant and any associated exemptions.

[15] The terms TDIF '*Accreditation Authority'* and '*Oversight Authority'* are used interchangeably between the TDIF and TDIF Interim MOU. Both terms refer to the same governance entity (Australian Govt Chief Digital Officer, DTA).

[16] As per the MOU - Accreditation Criteria means the criteria and requirements that a person applying to become accredited as Identity Exchange, a Credential Service Provider, an Identity Service Provider, or an Attribute Service Provider must meet (unless the Oversight Authority chooses to exempt any such criteria or requirement).

B.3 Process Map

Figure 1 provides an overview of the key steps in the process.

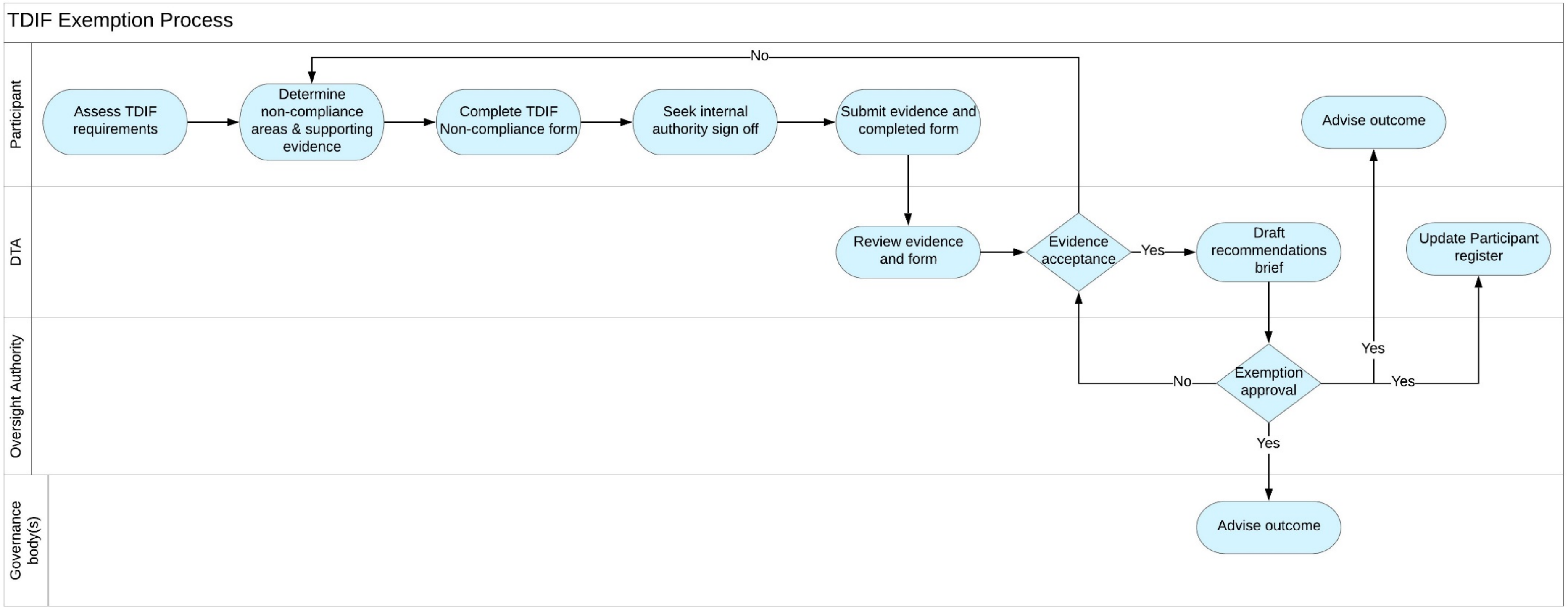

TDIF Exemption Process
Participant
DTA
Oversight Authority
Governance body(s)
Assess TDIF requirements
Determine non-compliance areas & supporting evidence
Complete TDIF Non-compliance form
Seek internal authority sign off
Submit evidence and completed form
No
Advise outcome
Review evidence and form
Evidence acceptance
Yes
Draft recommendations brief
Update Participant register
Exemption approval
No
Yes
Yes
Yes
Advise outcome

Figure 1 – TDIF exemption process

B.4 The exemption process

B.4.1 Evidence requirements

The TDIF includes a number of requirements, both foundation and supplementary, that Participants need to meet in order to achieve and maintain TDIF accreditation. Foundation requirements are applicable to all identity services. Supplementary requirements apply for specific identity services or in certain circumstances.

The TDIF Accreditation Process identifies what is to be provided as evidence by the Participant for their identity service. Appendix D details the compliance ratings that are to be used.

B.4.2 Non-Compliance determination

The Participant is required to review TDIF requirements and determine any areas of non-compliance. As part of their non-compliance determination activities the Participant is required to conduct a risk assessment, collect relevant evidence and record the impact of the non-compliance on both their identity service and (if known), on the federation. This information is to be included in a Non-Compliance form[17] that is to be submitted to their internal accreditation or certification authority for sign off.

B.4.3 Non-Compliance Form

Both the Participant's internal authority and the Oversight Authority can only make risk-based decisions if they are fully informed of the relevant facts. Without this information they cannot make an informed decision on whether to accept the residual risk and grant an exemption for a non-compliance request.

Participants seeking an exemption **MUST**:

- Document the justification for non-compliance against a TDIF requirement.
- Undertake a risk assessment.
- Document the alternative mitigation measures to be implemented, if any (including proposed date for remediation).

[17] See Appendix C for a template of the Non-Compliance Form that Participants should use when seeking an exemption against any TDIF requirement that has not been met.

- Specify the exemption period being sought.
- Obtain endorsement from internal certification authority of the non-compliance.

The Participant's Certification Authority is to endorse the proposed Non-Compliance Form. This endorsement also confirms the risk assessment outcomes and any proposed mitigation action and associated date for completion of the proposed action(s).

Where a Participant is non-compliant with multiple requirements for similar reasons, they may group these together in their report to simplify the reporting process.

Note: non-compliance with 'must' and 'must not' controls are likely to represent a high risk to information and systems. Non-compliance with 'should' and 'should not' controls are likely to represent a medium-to-low risk to information and systems. The Participant's internal accreditation or certification authority is able to consider the justification for non-compliance and advice on any associated residual risk to both the Participant and the federation.

B.4.4 Assessment Validation

Following this internal signoff, the Participant is required to submit their evidence and signed Non-Compliance form to the DTA for review.

Unless otherwise agreed between the Participant and the Oversight Authority all evidence provided to the DTA will be treated as Official information[18] and will be treated in accordance with the required level of security controls for their protection.

Upon receipt of the applicable evidence and signed Non-Compliance form, the DTA, including Subject Matter Experts (SME) as required, will review the Non-Compliance form and validate the evidence for compliance with TDIF requirements. The outcome of this review will be a determination of whether the evidence presented along with any proposed remediation(s) is acceptable and supports the Participant in meeting its accreditation obligations.

In order to maintain trust in the federation, the DTA, as required, may coordinate a federation risk assessment that may involve members of the DTA, applicable stakeholders (e.g. Accredited Providers) to review and assess the risk of the respective Participant's non-compliance impacts on the federation. The Participant will be actively involved in this process and may provide further information in regards to the non-compliance. Such information may include:

[18] NB. The outcomes of some accreditation may have a higher security classification and may not be shared with external parties; however, they must be made accessible to appropriate DTA members with a need to know.

- Elaboration and justification for non-compliance.
- Any mitigation measures that may have been implemented (or planned, including implementation date).
- An assessment of the risks relating to the federation.

The outcomes of this this activity will be a risk rating for the applicable non-compliances and an overall risk rating for the Participant’s identity service.

B.4.5 Accreditation conclusion

The DTA will form an opinion on the Participant’s exemption request and use this opinion to support the DTA’s brief sent to the Oversight Authority for consideration of the proposed exemption.

The DTA will draft a brief which recommends to the Oversight Authority to either accept or reject the proposed exemption. The Participant’s supporting evidence and signed Non-Compliance form will be provided to the Oversight Authority for their consideration as part of the brief.

Upon receipt of the brief and supporting documentation the Oversight Authority will decide whether to accept or reject the Participant’s exemption request. The outcome of this decision will be provided to the Participant.

If the request is accepted, the Participant will be granted an exemption against the relevant TDIF requirement. If the request is rejected, the Participant will not be granted an exemption and will be required to implement the TDIF requirement.

B.4.6 Updated Participants Register

All exemption requests and the Oversight Authority’s decisions will be recorded in the Participant Register.

The Oversight Authority may, at its discretion and in consultation with the Participant, advise other federation members of its decision to grant or reject an exemption request.

As the justification for non-compliance may change, and the risk environment will continue to evolve over time, it is important that Participants update their approval for non-compliance as part of their annual assessment activities. This allows the Oversight Authority to have review and exemption and either reaffirm or, if necessary, reject if the justification or residual risk is no longer acceptable.

Appendix C : TDIF Non-Compliance Request Template

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

Participant Name:	**Reference:**
Start Date:	**End Date:**
TDIF Document and Version:	
TDIF Requirement reference: **Control:** <Description>	
Applicability:	
Justification:	
Mitigation Measures: (implemented or planned – including dates)	
Alternative Mitigation Measures:	
Participant System Risk Assessment: {Risk Statements, Likelihood, Consequence, Risk Rating, Treatment(s), Recommended Treatment(s)}	
Federation Risk Assessment: {Risk Statements, Likelihood, Consequence, Risk Rating, Treatment(s), Recommended Treatment(s)}	
Participant POC:	
Participant Accreditation/Certification Authority Acknowledgement: **Printed Name:** **Signature:** **Date:**	
TDIF Oversight Authority Approval: **Printed Name:** **Signature:** **Date:**	

Appendix D : Compliance ratings

The Accredited Provider **MUST** use the following compliance ratings for the Requirements Self-Assertion to indicate whether the Accredited Provider continues to meet the TDIF requirements. Refer to the ISO 31000 or the Accredited Provider'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 Provider as their identity service 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 service supports other approved cryptographic algorithms instead).
- Compliant. The Accredited Provider has demonstrated with evidence they comply with a TDIF requirement or the intent of a requirement.
- Critical Non-Compliance. The Accredited Provider fails to meet a TDIF requirement which may result in Extreme unmitigated risk.
    - A Critical Non-Compliance **MUST** be classified as a critical failure and **MUST** result in a failed Self Assertion.
    - The withdrawal of an existing accreditation **MAY** occur until such time as the critical non-conformance is addressed.
- Major Non-Compliance. The Accredited Provider fails to meet a TDIF requirement which may result in High unmitigated risk.
    - A Major Non-Compliance **MUST** be classified as a major failure and **MUST** result in a failed Self Assertion.
    - Escalation of the problem to a critical failure **MUST** be imposed if additional events impact on the Accredited Provider simultaneously.
    - If the Accredited Provider fails to rectify the compliance problem within a timeframe agreed with the TDIF Accreditation Authority, 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 Provider 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 Provider fails to rectify the compliance problem within a timeframe agreed with the TDIF Accreditation Authority, 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 Provider 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 Provider fails to rectify the compliance problem within a timeframe agreed with the TDIF Accreditation Authority, then the status of the problem **MUST** be escalated to a partial failure where the conditions of that category are then applied.

Appendix E : Use of verified attributes outside the identity federation

E.1 Additional requirements on Identity Service Providers

If an Identity Service Provider wishes to allow an individual to verify identity to Relying Parties both inside the TDIF federation and outside the federation:

- It **MUST** notify the TDIF Oversight Authority of any identity services provided (at the time of accreditation and if new services are supported) outside the TDIF federation that leverage identities that are created and used in the TDIF federation.
- It **MUST** ensure it provides clear information to individuals and Relying Parties when the identity services it provides are used within the TDIF federation and when its identity services are being provided outside the TDIF federation.
- When it provides identity services outside the TDIF federation the Identity Service Provider **MUST** advise users that the services it is providing do not comply to the TDIF requirements and is being used outside the TDIF federation.
- It **MUST** notify the TDIF Oversight Authority of any privacy, protective security or fraud incidents or risks identified in the use of identities outside the TDIF federation that may affect privacy, security or fraud capabilities of the TDIF federation.

E.2 Additional requirements on Attribute Providers

If an Attribute Provider wishes to allow an individual to share attributes to Relying Parties both inside the TDIF federation and outside the federation:

- It **MUST** notify the Oversight Authority of any provision of attribute services (at the time of accreditation and if new services are supported) outside the TDIF federation that leverage attributes that are used in the TDIF federation.
- It **MUST** ensure it is clear to users and Relying Parties when the attribute services it provides are being used within the TDIF federation and when these services are being provided outside the TDIF federation.
- When it provides attribute services outside the TDIF federation the Attribute Provider **MUST** advise individuals and Relying Parties that the services it provides do not comply with the TDIF requirements and are being used outside of TDIF federation.

- It **MUST** notify the Oversight Authority of any privacy, security or fraud incidents or risks identified in the use of attributes outside the TDIF federation that may affect privacy, security and fraud capabilities of the TDIF federation.

Appendix F : Restricted Attributes

An Identity Service Provider is required to collect and verify an individual's identity information as part of performing its identity management function. The permissible attributes that can be collected and disclosed to Relying Parties are defined in section 2 (2.2.1 through 2.2.4) of the *TDIF: Attribute Profile* (v1.4, Mar 2019).

In accordance with section 2.2.8.1 of the *TDIF: Attribute Profile* (v1.4, Mar 2019), an Identity Service Provider is permitted to disclose additional *restricted attributes*[19] to a Relying Party where the Relying Party meets the following requirements:

- The disclosure of restricted attributes will satisfy a specific legislative or regulatory requirement applicable to the Relying Party. Prior to obtaining the restricted attributes the Relying Party must adequately satisfy all inquiries of the TDIF Oversight Authority regarding their need for restricted attributes. This may require the Relying Party to provide evidence of their legislative or regulatory requirements to the TDIF Oversight Authority and how they will be met by obtaining these restricted attributes. The Relying Party will not be approved to obtain these restricted attributes if it fails to adequately justify its need to the TDIF Oversight Authority.
- The restricted attributes requested by the Relying Party cannot exceed those which are collected by the Identity Service Provider as part its normal operation.
- The Relying Party can demonstrate its protective security, privacy and fraud control arrangements are effective and working as intended. A Relying Party will not be approved to obtain restricted attributes if it fails to demonstrate effective risk management governance that includes an appropriate internal management structure and oversight arrangements for managing risk.

The TDIF Oversight Authority will advise the Relying Party whether it has satisfied the above requirements and is approved to request restricted attributes.

Where the TDIF Oversight Authority determines the Relying Party has satisfied the above requirements it will:

- Advise the Relying Party and all relevant stakeholders, including Identity Service Providers, that the Relying Party has been granted approval to request restricted attributes.
- All Identity Service Providers **MUST** enable the disclosure of these restricted attributes.
- The disclosure of restricted attributes **MUST** occur with the consent of the individual.

[19] *Restricted attributes* include identity credential identifiers and other identity credential information (e.g. validity period, credential issuer).

Where the TDIF Oversight Authority determines the Relying Party has not satisfied the above requirements it will advise the Relying Party accordingly and state the reasons why their request for restricted attributes has not been approved.