Australian Government
Digital Transformation Agency

03 - Accreditation Process

Trusted Digital Identity Framework Release 4
May 2020, version 1.0

PUBLISHED VERSION

Digital Transformation Agency (DTA)

Licence

Use of the Coat of Arms

Conventions

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

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

Contact us

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

Document management

The *DTA* has endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.1	Aug 2019	SJP	Initial version
0.2	Sep 2019	SJP	Updated to incorporate feedback provided by stakeholders during the first round of collaboration on TDIF Release 4
0.3	Dec 2019	SJP	Updated to incorporate feedback provided by stakeholders during the second round of collaboration on TDIF Release 4
0.4	Mar 2020	SJP	Updated to incorporate feedback provided during the public consultation round on TDIF Release 4
1.0	May 2020		Published version

Document review

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

Contents

List of Figures

1 Introduction

This document sets out the *TDIF Accreditation Process* which involves a combination of documentation requirements, third party evaluations and operational testing that *Applicants* must complete to the satisfaction of the *DTA* to achieve *TDIF* accreditation. The intent of accreditation is to determine whether the *Applicant's* identity system meets the requirements set out in the *TDIF*.

The intended audience for this document includes:

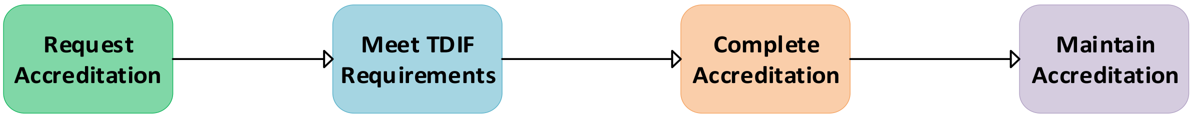
- *Accredited Participants*.
- *Applicants*.
- *Assessors.*
- *Relying Parties*.

2 TDIF Accreditation Process

2.1 Overview

The *TDIF Accreditation Process* is a formal process through which *Applicants* demonstrate their ability to meet the accreditation requirements to the satisfaction of the *DTA*. Figure 1 provides an overview of the *TDIF Accreditation Process*.

Figure 1: TDIF Accreditation Process.



The three accreditation processes, ‘Request Accreditation, Meet TDIF Requirements’ and ‘Complete Accreditation’ are the focus of this document. The fourth accreditation process, ‘Maintain Accreditation’ is the focus of the document titled *TDIF: 07 - Annual Assessment*.

Progress through the *TDIF Accreditation Process* is managed by a series of decision gates. The decision gates are used by the *DTA* to evaluate the *Applicant’s* progress towards *TDIF* accreditation and their ability to meet ongoing accreditation obligations. Arrows show the relationships between accreditation activities. All activities can be iterated.

The *DTA* expects the *Applicant* to understand the requirements, compliance obligations and likely costs associated with pursuing accreditation before commencing the *TDIF Accreditation Process*.

This document does not define maximum periods that individual activities, or the *TDIF Accreditation Process* is likely to take as this is largely driven by the *Applicant***.** The *Applicant* should be able to achieve *TDIF* accreditation within 12 months of submitting a *TDIF Application Letter* to the *DTA*. Factors that impact on the time taken to complete an activity or achieve accreditation include:

- The *Applicant's* understanding of the *TDIF Accreditation Process* and *TDIF* requirements.
- The nature and maturity of the identity system being accredited.
- The *Applicant's* business needs, threat environment and risk tolerance.
- The degree to which the *Applicant's* identity system is straightforward, easy to use, secure and privacy preserving.
- The time taken by the *Applicant* to complete the required *Functional Assessments* from *Assessors* and address any non-compliance issues to the satisfaction of the *DTA*.

An *Applicant* with a fully operational identity system who is familiar with the *TDIF* requirements is 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 system.

All costs associated with *TDIF* accreditation are to be met by the *Applicant*. For example, to pay for an Assessor for the *Privacy Impact Assessment* (PIA) or security assessment. 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 an *Assessor*.

The *DTA* does not maintain a list of approved *Assessors*. As part of good corporate governance, the *Applicant* should be able to identify and obtain appropriate resources with the relevant skills, experience, independence and qualifications to undertake the *Functional Assessments*.

TDIF accreditation can be sought by *Applicants* that:

- Participate in the open market and choose to undergo the *TDIF Accreditation Process* to increase the perceived assurance of their identity. This includes organisations that operate their own identity system (single entity) and organisations that provide components of an identity system that work together (multi-entity).
- Are members of an existing community of interest and choose to undergo the *TDIF Accreditation Process* to increase the perceived assurance of their identity system to other members of the community of interest.

- Are required to meet the *TDIF* prior to joining the *Australian Government's identity federation*.

An *Applicant* can apply to undergo the *TDIF Accreditation Process* at any stage in the development life cycle of their identity system, however, the *DTA* will only grant accreditation to a fully operational identity system which meets all applicable *TDIF* requirements. The *DTA* will not grant partial accreditations.

Successful completion of the *TDIF Accreditation Process* will result in the organisation being listed on the *DTA* website[1] as an *Accredited Participant*.

Once accredited, the *Accredited Participant* is required to demonstrate its ability to maintain *TDIF* accreditation. Each year the *Accredited Participant* is required to complete an *Annual Assessment* by the anniversary of its initial accreditation date.

Following accreditation, the *Accredited Participant* may be directed by the *DTA* to undergo *TDIF Reaccreditation* following a cyber security or fraud incident, or serious or repeated breaches related to privacy or data, or as a result of a changing threat or operating environment which materially impacts the identity system risk profile. If *TDIF Reaccreditation* is required, the *DTA* will determine whether it replaces the requirement for the *Accredited Participant's Annual Assessment*.

2.2 Previous functional assessments

In accordance with the *TDIF*: *04 - Functional Requirements,* the *Applicant's* identity system is required to undergo *Functional Assessments* by *Assessors*. These *Functional Assessments* cover protective security, privacy, accessibility and usability.

Applicants may have recently undergone assessments on their identity system which cover similar requirements to those listed in *TDIF*. The *Applicant* may, as per its *TDIF Application Letter*, submit evidence of assessments conducted in the previous 12 months and request the *DTA* consider it as a substitute for a *Functional Assessment*.

[1] See the *DTA* website on the *TDIF* for further information on *Accredited Participants*.

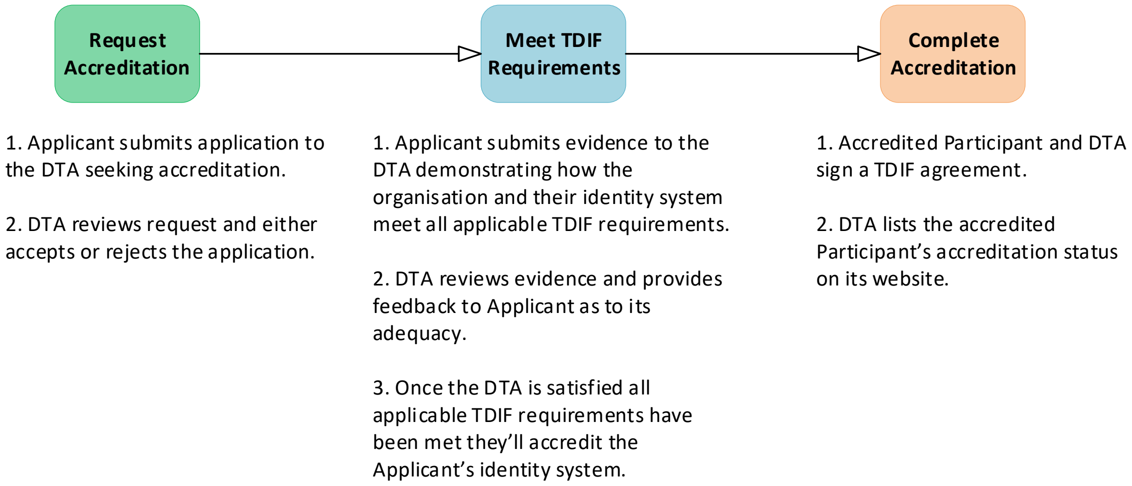
At its discretion, the *DTA* may accept prior assessments conducted on the *Applicant's* identity system as a substitute to a *Functional Assessment* required by the *TDIF*. In such instances the *DTA* will advise the *Applicant* in writing the adequacy of prior assessments relative to the degree to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

- Fully addresses a *Functional Assessment* then no further action will be required by the *Applicant* for that *Functional Assessment*.
- Partially addresses a *Functional Assessment* then the *Applicant* will need to undergo a partial *Functional Assessment* for the requirements it does not meet.
- Does not address a *Functional Assessment* then the *Applicant* will need to undergo the *Functional Assessment* as described in the *TDIF*: *04 - Functional Requirements*.

3 TDIF accreditation activities

Figure 2 lists the three major activities required to complete *TDIF* initial accreditation as well as a high-level description of these activities.

Figure 2: TDIF accreditation activities.



1. Applicant submits application to the DTA seeking accreditation.

2. DTA reviews request and either accepts or rejects the application.

1. Applicant submits evidence to the DTA demonstrating how the organisation and their identity system meet all applicable TDIF requirements.

2. DTA reviews evidence and provides feedback to Applicant as to its adequacy.

3. Once the DTA is satisfied all applicable TDIF requirements have been met they'll accredit the Applicant's identity system.

1. Accredited Participant and DTA sign a TDIF agreement.

2. DTA lists the accredited Participant's accreditation status on its website.

3.1 Request Accreditation

The 'Request Accreditation' activity requires the *Applicant* to request *TDIF* accreditation in accordance with the requirements of this section.

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

The *Applicant* *MUST* formally request *TDIF* accreditation and complete the *TDIF Application Letter* at Appendix A[2].

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

The *TDIF Application Letter* *MUST* specify *Accredited Roles* being sought, or a combination of these.

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

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

The *TDIF Application Letter* *MUST* specify the assurance levels supported by their identity service. For *Identity Service Providers* this means *Identity Proofing Levels*. For *Credential Service Providers* this means *Credential Levels*[3].

TDIF Req: ACCRED-03-01-02b; **Updated**: Mar-20; **Applicability**: C, I

The *TDIF Application Letter* *MUST* specify whether the identity system supports web responsive design, mobile apps or a combination of these. This information will determine the accessibility assessment to be met.

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

The Application Letter *MUST* include a *Statement of Applicability* which lists the protective security controls implemented by the *Applicant* for their identity system.

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

At a minimum, the *Statement of Applicability* *MUST*:

a) Specify the *Applicant's* risk tolerance for their identity system.

b) Be written for an operational identity system, regardless of whether the *Applicant's* identity system is operational or not.

c) Include all protective security requirements (section 4) set out in *TDIF: 04 - Functional Requirements*.

d) Include the version of the *Australian Government Information Security Manual* used as its basis (i.e. month and year).

The *Statement of Applicability* forms the basis of the *Applicant's* security assessment.

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

For multi-entity identity systems, the *Statement of Applicability* *MUST* include all protective security controls which directly contribute to meeting *TDIF* protective security requirements.

TDIF Req: ACCRED-03-01-04; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *TDIF Application Letter* *MUST* include an accreditation schedule which highlights key dates and accreditation milestones.

TDIF Req: ACCRED-03-01-04a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *TDIF Application Letter* *MUST* propose a date by which *TDIF* accreditation is anticipated[4].

[3] See the *TDIF: 05 - Role Requirements* for further information on *Identity Proofing* and *Credential Levels*.

[4] Based on *DTA* experience, the average time to complete the *TDIF Accreditation Process* ranges from 9 – 12 months.

TDIF Req: ACCRED-03-01-05; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *TDIF Application Letter* *MUST* include the names and contact details of people responsible within the *Applicant's* organisation to manage their *TDIF* accreditation[5].

TDIF Req: ACCRED-03-01-06; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *TDIF Application Letter* *MAY* include any relevant *TDIF Exemption Requests* in accordance with the process set out in 'Appendix B: TDIF exemption process'.

TDIF Req: ACCRED-03-01-06a; **Updated**: Mar-20; **Applicability**: A, C, I, X
Each *TDIF Exemption Request* *MUST* include all information as described in 'Appendix B: TDIF exemption process'.

TDIF Req: ACCRED-03-01-07; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MAY* include a copy of prior assessments which it requests the *DTA* consider as a substitute for relevant *Functional Assessments*.

On receiving a *TDIF Application Letter*, the DTA will acknowledge the *Applicant's* request to undergo the *TDIF Accreditation Process* in writing. The *DTA* will subsequently review the *TDIF Application Letter* and supporting information. The *DTA* will either:

- Approve the *Applicant's* request to continue with *TDIF* accreditation activities where the *DTA* is satisfied with the information provided in the *TDIF Application Letter* by the *Applicant*. In such instances the *DTA* will advise the *Applicant* of its decision; or
- Reject the *Applicant's* request to continue with *TDIF* accreditation if the *DTA* is not satisfied with the information provided in the *TDIF Application Letter* by the *Applicant*. Where a request for *TDIF* accreditation has been rejected, the *DTA* will advise the *Applicant* of its decision, the reasons why and the actions to be taken by the *Applicant* for their *TDIF Application Letter* to be reconsidered by the *DTA*.

[5] The *DTA* recommends a central person or area be responsible within the *Applicant's* organization to manage their *TDIF* accreditation. This will greatly aide in coordination and management of accreditation activities.

3.2 Meet TDIF Requirements

The ‘Meet TDIF Requirements’ activity requires the *Applicant* to demonstrate how it and its identity system meet all applicable *TDIF* requirements.

3.3 Complete Accreditation

Upon successfully completing the ‘Meet TDIF Requirements’ activity, the *Applicant* and its identity system will be listed on the *DTA’s* website as an *Accredited Participant* and the *DTA* will update the *TDIF Accreditation Register*.

Following accreditation, the *Accredited Participant* must, if required by the *DTA*, enter into an agreement with the *DTA* which sets out the rights, roles and obligations of both parties in relation to the *Accredited Participant’s TDIF* accreditation.

The *Accredited Participant* is required to undergo an *Annual Assessment* by the anniversary of their initial accreditation date. Further information on the *Annual Assessment* is set out in the *TDIF: 07 - Annual Assessment.*

Appendix A: TDIF Application Letter template

[Applicant's letterhead]

[date]

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]* is seeking 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]* as [*web responsive, mobile app, or a combination of these*] 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 or is not Australian owned and provide your ABN].

At this stage we expect to commence accreditation by *[date]* and anticipate completing all accreditation activities by *[date].* Attached is our accreditation schedule and list of key personnel who will lead our accreditation efforts. *[don't forget to include the accreditation schedule or list of key personnel]*

Also attached is our Statement of Applicability. *[don't forget to attach the Statement of Applicability]*

Finally, we request our prior audit work be considered as a substitute to meeting the TDIF functional assessments. The reason for this is [provide justification]. [*don't forget to attach prior audit or assessment work]*

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 Appendix outlines the process to be used by an *Applicant* when seeking an exemption against a *TDIF* requirement. Prior to submitting to the *DTA*, an exemption request:

- Is to be signed off by the *Applicant's* relevant *Accountable Authority*.
- Is to include a completed and signed *TDIF Exemption Request* form in the form set out in section B.2.6.
- Is to be supported with relevant evidence.

Figure 3 provides an overview of the key steps in the process.

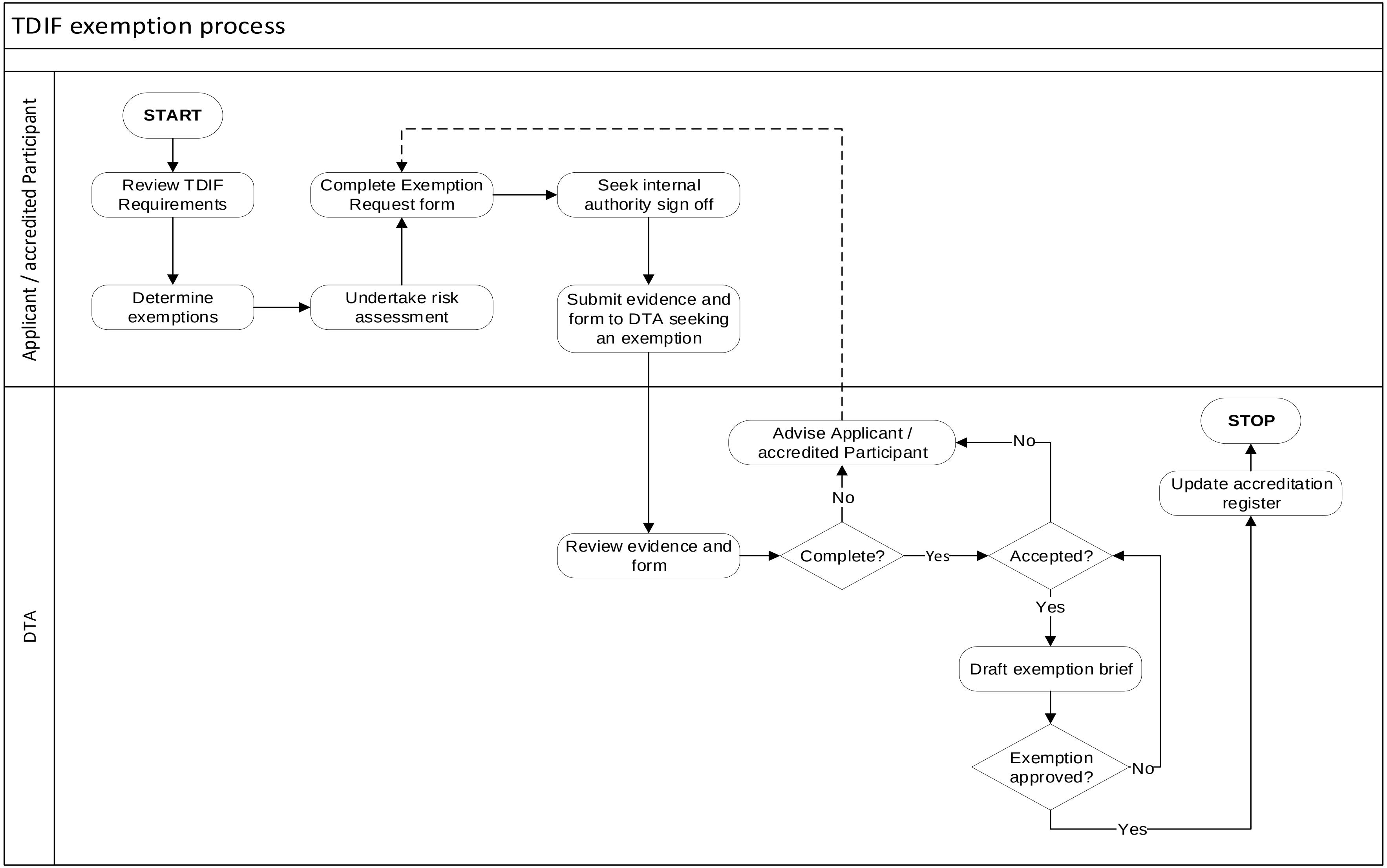

TDIF exemption process
Applicant / accredited Participant
DTA
START
Review TDIF Requirements
Determine exemptions
Undertake risk assessment
Complete Exemption Request form
Seek internal authority sign off
Submit evidence and form to DTA seeking an exemption
Review evidence and form
Complete?
Yes
No
Advise Applicant / accredited Participant
Accepted?
No
Yes
Draft exemption brief
Exemption approved?
No
Yes
Update accreditation register
STOP

Figure 3: TDIF exemption process.

B.2 Exemption activities

B.2.1 Exemption determination

The *Applicant* is required to review all applicable *TDIF* requirements and determine the impacts of meeting them. Where compliance with a *TDIF* requirement would negatively impact their identity system, the *Applicant* may determine relevant exemptions[6]. The *Applicant* is required to conduct a risk assessment on the proposed exemptions and collect relevant evidence which supports the exemption request. This information is to be included in a *TDIF Exemption Request* form (see below) that is to be submitted to the *Applicant's Accountable Authority*[7] for approval.

B.2.2 Exemption request form

The *Applicant's Accountable Authority* and the *DTA* can only make risk-based decisions if they are fully informed of the relevant facts. Without this information it cannot make an informed decision on whether to grant an exemption against a *TDIF* requirement.

Applicants seeking an exemption are required to:

- Complete the *TDIF Exemption Request* form in the form set out in section B.2.6.
- Document the justification for exemption against a *TDIF* requirement.
- Undertake a risk assessment.
- Document the alternative mitigation measures to be implemented, if any (including proposed date for remediation).
- Specify the exemption period being sought.
- Obtain endorsement from an appropriate *Accountable Authority* for the non-compliance.

[6] The *DTA* will generally support an exemption request where the *Applicant* can demonstrate the request is required to support business needs or address likely, realistic and probable risks. The *DTA* will not support an exemption request where the *Applicant* simply chooses not to meet a *TDIF* requirement.

[7] Typically, the *Accountable Authority* within the *Applicant's* organization is the business area responsible for managing the subject matter under question.

If supported, the *Applicant's Accountable Authority* is required to sign the *TDIF Exemption Request* 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 an *Applicant* is seeking an exemption against multiple *TDIF* requirements for similar reasons, it may group these together in their report to simplify the reporting process.

B.2.3 Assessment validation

Following this internal signoff, the *Applicant* is required to submit its evidence and signed *TDIF Exemption Request* form to the *DTA* for review. The *DTA* will initially review the *TDIF Exemption Request* to ensure all required information has been provided. The *DTA* will then consider the request along with the evidence. The outcome of this review will be a determination of whether the evidence presented along with any proposed remediations are acceptable and supports the *Applicant* in meeting its *TDIF* accreditation obligations.

Unless otherwise agreed between the *Applicant* and the *DTA*, all evidence provided to the *DTA* will be treated as *OFFICIAL information*[8].

B.2.4 Accreditation conclusion

The *DTA* will form an opinion on the *Applicant's TDIF Exemption Request* and supporting evidence. Upon receipt of the brief and supporting documentation the *DTA* will decide whether to accept or reject the *Applicant's TDIF Exemption Request*. The outcome of this decision will be provided to the *Applicant*.

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

B.2.5 Update accreditation register

All *TDIF Exemption Requests* and the *DTA's* decisions will be recorded in the *TDIF Accreditation Register*.

The *DTA* may, at its discretion and in consultation with the *Applicant*, advise other *Participants* of its decision to grant or reject a *TDIF Exemption Request*.

[8] NB. Some *TDIF* accreditation activities may have a higher security classification and may not be shared with external parties; however, they must be made available to appropriate *DTA* personnel with a need to know.

As the justification for exemptions may change, and the risk environment will continue to evolve over time, it is important that *Applicants* 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.

B.2.6 TDIF Exemption Request form template

Refer to the *ISO* 31000 or the *Applicant'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:		
Applicability [A, C, I, X]:		
Justification for exemption request:<Description>		
Mitigation measures: (implemented or planned – including dates)		
Alternative mitigation measures:		
Applicant system risk assessment: {Risk Statements, Likelihood, Consequence, Risk Rating, Treatment(s), Recommended Treatment(s)}		
Applicant point of contact:		
Applicant internal authority approval: **Printed Name:**	 **Signature:**	 **Date:**
DTA Approval: **Printed Name:**	 **Signature:**	 **Date:**