



Digital Identity

TDIF Variation – Standard Operating Procedure

Trusted Digital Identity Framework

May 2022, document version 1.1

PUBLISHED VERSION



Digital Transformation Agency (DTA)

This work is copyright. Apart from any use as permitted under the Copyright Act 1968 and the rights explicitly granted below, all rights are reserved.

Licence



With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (<http://creativecommons.org/licenses/by/4.0/legalcode>)

This licence lets you distribute, remix, tweak and build upon this work, even commercially, as long as they credit the DTA for the original creation. Except where otherwise noted, any reference to, reuse or distribution of part or all of this work must include the following attribution:

Trusted Digital Identity Framework (TDIF)™ © Commonwealth of Australia (Digital Transformation Agency) 2022

Use of the Coat of Arms

The terms under which the Commonwealth Coat of Arms can be used are detailed on the It's an Honour website (<http://www.itsanhonour.gov.au>) Conventions References to TDIF documents, abbreviations and key terms (including the words MUST, MUST NOT, and MAY) are denoted in italics are to be interpreted as described in the current published version of the *TDIF: 01 – Glossary of Abbreviations and Terms*.

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

Contact us

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

Document management

The DTA has endorsed this document for release.

Change log

Document Version	Date	Author	Description of the <i>changes</i>
0.1	Dec 2020	<i>Digital Identity Policy</i>	Overview drafted
1	Dec 2020	<i>Digital Identity Policy</i>	Published version
1.1	May 2022	JK	Updated with current processes

Contents

Glossary of terms	iii
Executive Summary	1
1 Change Request Management	3
2 Policy Release Train Process	4
2.1 Emergency Change Process	4
2.2 Material Change Process.....	4
2.3 Routine Change Process	4
3 Stakeholder Consultation	6
4 Finalisation	8

Glossary of terms

Change. A variation made to the *TDIF*.

Change Backlog. The list of approved *Changes* yet to be actioned by the DTA.

Change Log. The official record of *TDIF* version *Changes* published on the Digital Identity website.

Change Priority. The priority assigned to a *Change Request* (i.e. *Emergency Change*, *Material Change* or *Routine Change*).

Change Register. Records all activities and decisions relating to an individual *Change Request* including: *Change Request form*, *sign off*, Consultation Requests and Finalisation.

Change Request. A request submitted by a *Change Requestor* seeking a variation to the *TDIF*. Each *Change Request* is documented using a *Change Request Form* and will either be accepted or rejected by the DTA.

Change Request Form. The change request form is a PDF document available on the *TDIF* website¹ that has fields for all the information required for a change to be assessed and processed.

Change Request Management Process. The Change Request Management Process ensures all *Change Requests* are actionable, categorised, acknowledged, uniquely trackable and interpreted and actioned consistently.

Change Summary Record. Refers to the record of all activities and decisions relating to *Changes* across all documentation.

Digital Identity Policy. The DTA team responsible for developing, updating and maintaining the *TDIF*.

Emergency Change. Means an immediate *change* is required to correct a grammatical error or other error, or factual inaccuracy which directly affects

¹ <https://www.digitalidentity.gov.au/tdif>

accreditation effort or the integrity of the *TDIF*. *Emergency Changes* do not undergo consultation before being incorporated into the *TDIF*.

Interim Oversight Authority (IOA). The authority that provides Digital Identity Oversight services until Legislation is put in place.

Material Change. Denotes a *change* to a document that sets out *TDIF* requirements. All Material Changes undergo consultation before being incorporated into the *TDIF*. Material Changes apply to the following *TDIF* documents:

- *TDIF 03 Accreditation Process*
- *TDIF 04 Functional Requirements*
- *TDIF 05 Role Requirements*
- *TDIF 06 Federation Onboarding Requirements*
- *TDIF 06B OpenID Connect Profile*
- *TDIF 06C SAML 2.0 Profile*
- *TDIF 07 Maintain Accreditation.*

Policy Release Train Process. Refers to the process of drafting, QA, Stakeholder Consultation subprocess and *Sign off* for categorised *TDIF* Changes. *Emergency*, *Material* and *Routine Changes* have different required Policy Release Train Processes.

Routine Change. Denotes a *change* to a document that does not set out *TDIF* requirements. Routine Changes may undergo consultation—as deemed required by the *Digital Identity Policy* team—before being incorporated into the *TDIF*. Routine Changes apply to the following *TDIF* documents:

- *TDIF 01 Glossary of Abbreviations and Terms*
- *TDIF 02 Overview*
- *TDIF 04A Functional Guidance*
- *TDIF 05A Role Guidance*
- *TDIF 06A Federation Onboarding Guidance*
- *TDIF 06D Attribute Profile*

Sign off. By the appropriate delegate is required for *Emergency*, *Routine* and *Material changes*. Approvals required:

- i. **Emergency:** Director of *Digital Identity Policy* and Accreditation (EL2)
- ii. **Routine:** Branch Manager, Digital Identity (SES1)
- iii. **Material:** General Manager of Digital Discovery and Sourcing (SES2)

Trusted Digital Identity Framework (TDIF). Sets out the requirements that applicants need to meet to achieve TDIF accreditation. The TDIF also includes guidance material and templates to support providers to meet TDIF requirements. The TDIF accreditation requirements cover privacy, protective security, accessibility and usability, risk management, records management, fraud control, technical testing, and identity proofing and authentication credential management.

Executive Summary

The *TDIF* Variation - Standard Operating Procedure (SOP) sets out the approach to make changes to the *TDIF*. It includes the steps to follow when assessing, prioritising and actioning changes to the *TDIF*.

Anyone can request a change to the *TDIF* via the *Change Request Form* on the Digital Identity website².

The majority of *TDIF* changes and *Change Requests* will likely be generated from:

- Digital Identity program stakeholders
- Changes to legislation which impact the *TDIF* (e.g. the development of Digital Identity legislation)
- The staff of jurisdiction government agencies
- Agencies and organisations that undergo *TDIF* accreditation.

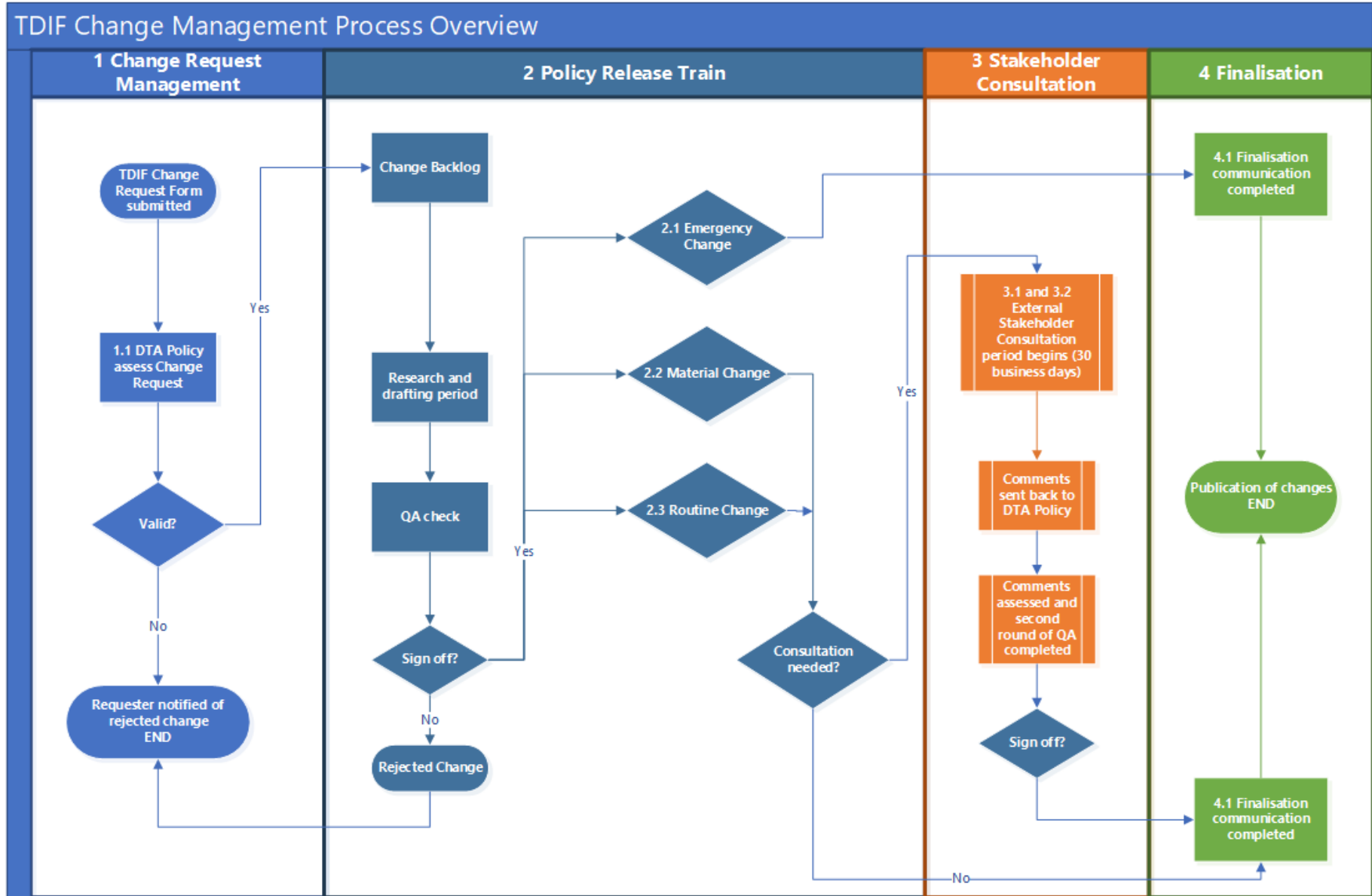
The *TDIF Variation SOP* ensures all *changes* to the *TDIF* are managed in a consistent manner. The *Change Management Process* encompasses internal documents and registers to track changes to the *TDIF* and ensures that archiving of the *TDIF* versions is completed appropriately.

The Change Management Process is broken down into four steps:

1. **Change Request Management:** ensures all *Change Requests* are actionable, categorised, acknowledged, uniquely trackable and interpreted and actioned consistently.
2. **Policy Release Train:** the schedule of drafting, QA, *Sign off*, Consultation, and Finalisation for *TDIF* changes that will be published as required.
3. **Stakeholder Consultation:** All *Material Changes* must undergo stakeholder consultation for a mandatory period of 30 *Business Days*.
4. **Finalisation:** the last step before the *Changes* are published on the *TDIF* website.

Below is an overview of the *TDIF* Change Management Process.

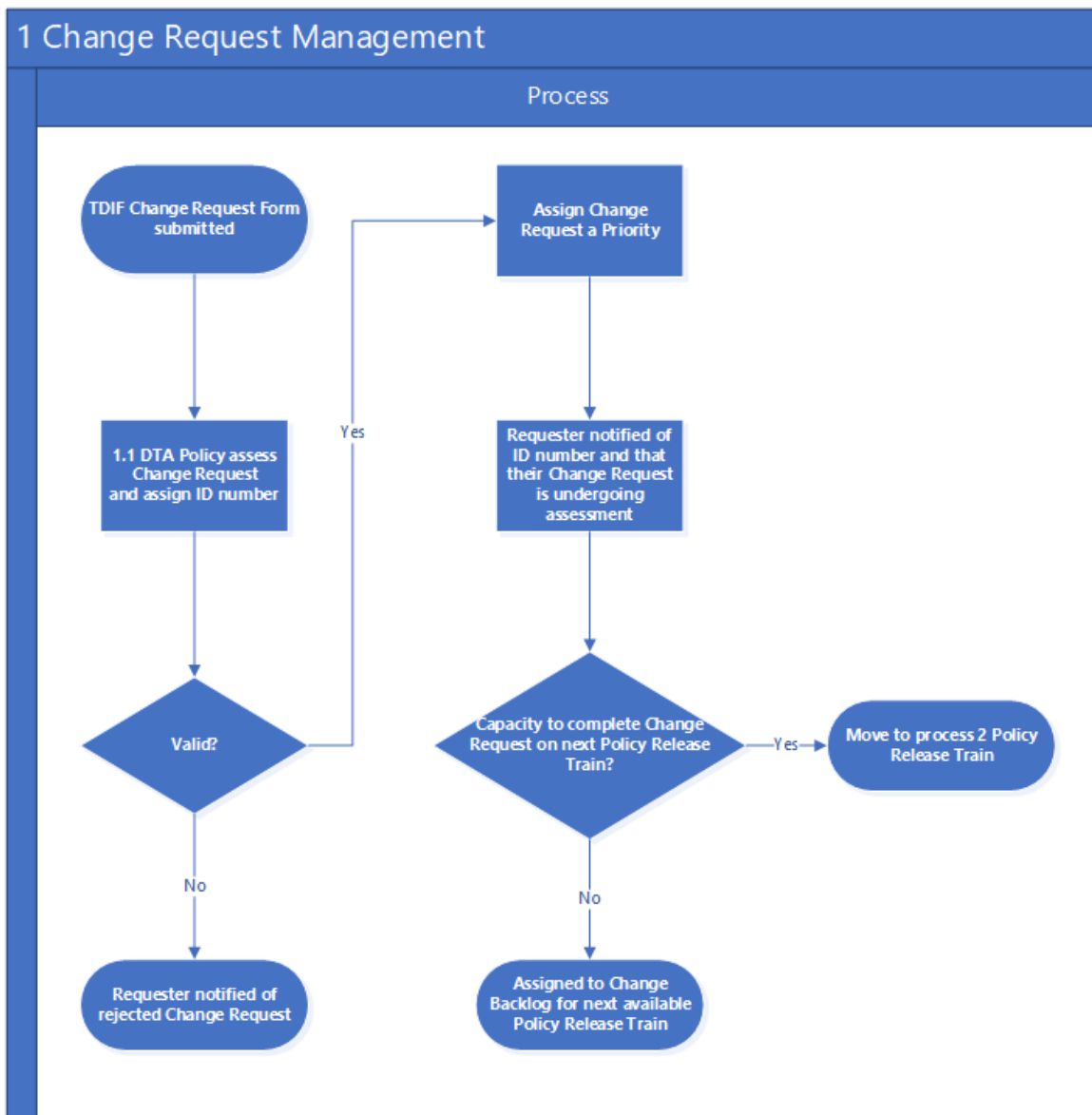
² [Trusted Digital Identity Framework \(TDIF\) | Digital Identity](#)



1 Change Request Management

The *Change Request Management Process* ensures all *Change Requests* are actionable, categorised, acknowledged, uniquely trackable, interpreted and actioned consistently.

A change to the *TDIF* can be requested by filling out a *Change Request form*, located on the *TDIF* website, and emailing it to digitalidentity@dta.gov.au



2 Policy Release Train Process

2.1 Emergency Change Process

An *Emergency Change* is an immediate *change* to the TDIF to correct a grammatical or other error, or factual inaccuracy which directly affects accreditation effort or the integrity of the *TDIF*. *Emergency Changes* do not undergo consultation before being incorporated into the *TDIF*. *Emergency Changes* are scheduled for publication on or around the first Business Monday of each month, as required.

2.2 Material Change Process

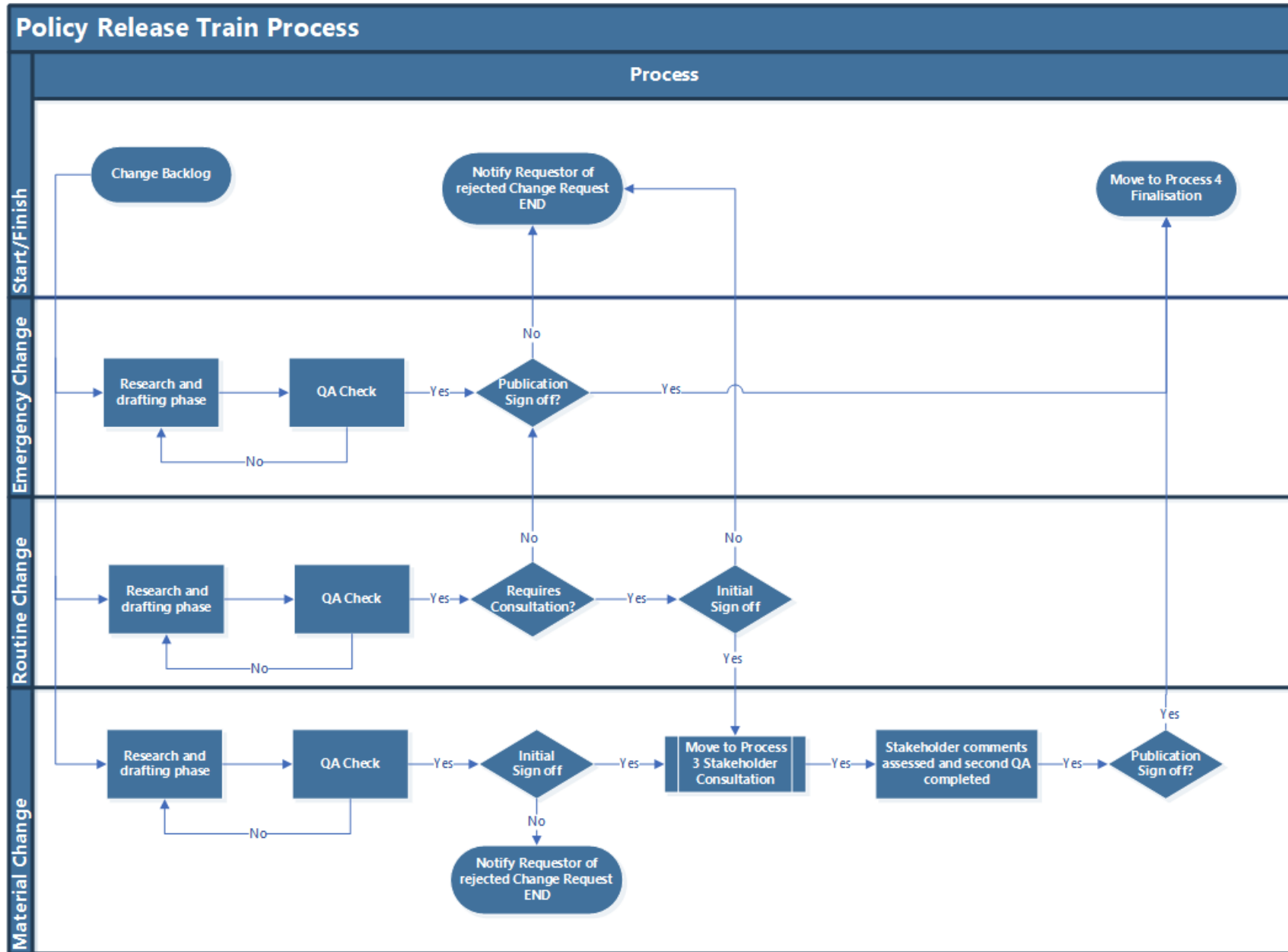
Material Changes are changes to the *TDIF* requirements. All Material Changes undergo mandatory 30 business day consultation with stakeholders before being incorporated into the *TDIF*. Material Changes apply to the following *TDIF* documents:

- TDIF 03 Accreditation Process
- TDIF 04 Functional Requirements
- TDIF 05 Role Requirements
- TDIF 06 Federation Onboarding Requirements
- TDIF 06B OpenID Connect Profile
- TDIF 06C SAML 2.0 Profile
- TDIF 07 Maintain Accreditation.

2.3 Routine Change Process

Routine Changes are changes to all other TDIF documents that do not include *TDIF* requirements. Routine Changes may undergo consultation—as deemed required by the *Digital Identity Policy* team—before being incorporated into the *TDIF*. Routine Changes apply to the following *TDIF* documents:

- TDIF 01 Glossary of Abbreviations and Terms
- TDIF 02 Overview
- TDIF 04A Functional Guidance
- TDIF 05A Role Guidance
- TDIF 06A Federation Onboarding Guidance
- TDIF 06D Attribute Profile



3 Stakeholder Consultation

All *Material* and some *Routine Changes* will undergo stakeholder consultation for a mandatory period of 30 Business Days. The broad groups of stakeholders simultaneously consulted during this time are:

- Accredited Providers listed on the *TDIF* website that have achieved *TDIF* accreditation.
- Members of the Interim Oversight Authority (IOA) forum.
- The Digital Identity Cross Jurisdictional Working Group³.
- Applicants undergoing *TDIF* accreditation.

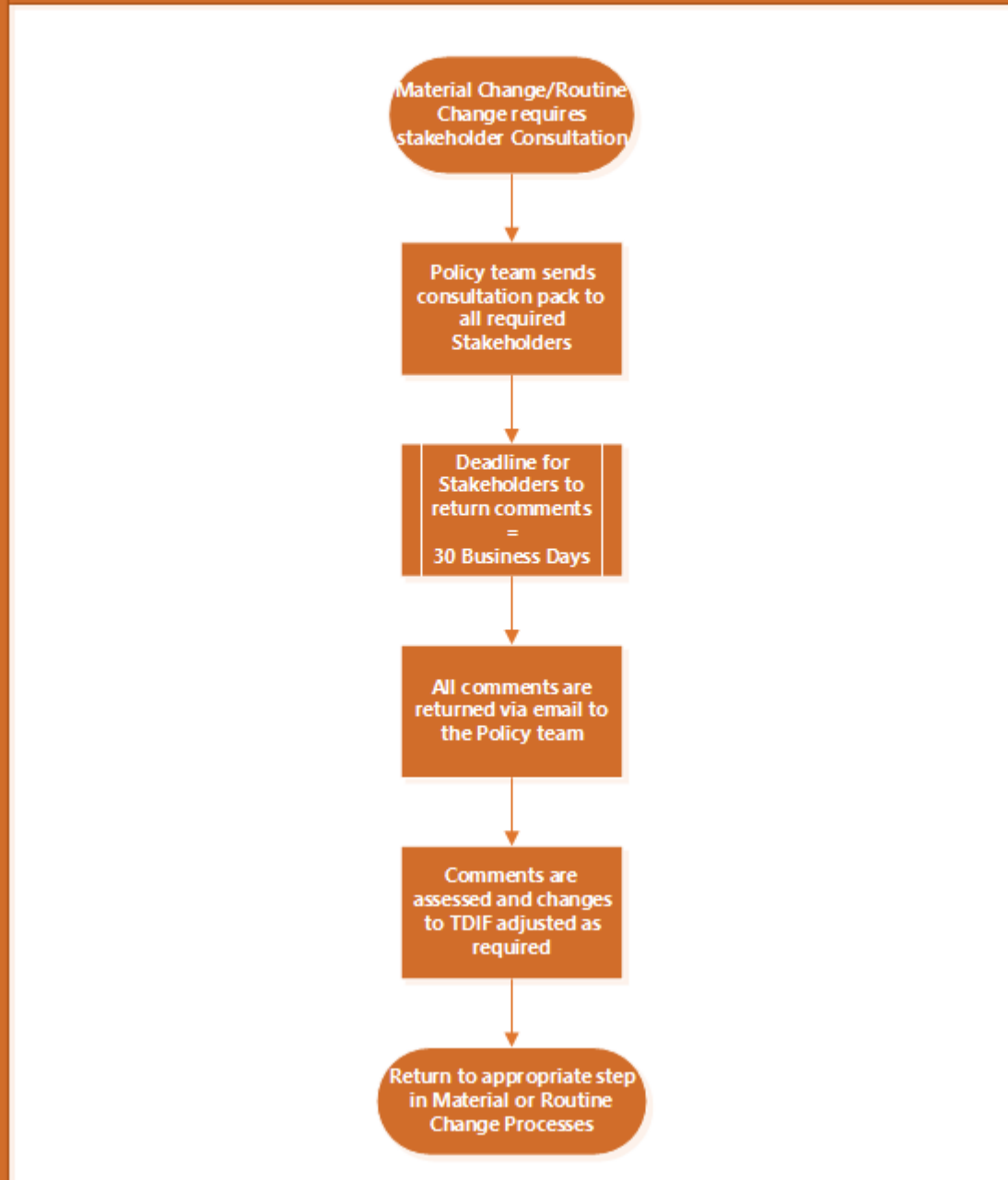
Depending on the nature of the *Change*, other individuals, organisations and agencies may also be consulted during the 30 *Business Day* period, including:

- Other Australian Government agencies (e.g Home Affairs).
- Parties which have established Digital Identity Mutual Recognition arrangements with Australia.
- Subject matter experts (e.g. biometrics specialists).

³ The DICJWG is a working group which reports through the Senior Officials Group to the Australian Data and Digital Council.

3 Stakeholder Consultation

Process



4 Finalisation

Finalisation is the last step before the *TDIF* Changes are published, as required by the *Policy Release Train*. All changes are quality assurance checked and signed off for publication on the Digital Identity website. Stakeholders will be notified of a TDIF change upon publication.

