Australian Government
Digital Transformation Agency

Accreditation Process

Trusted Digital Identity Framework
February 2018, version 1.0

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

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 regarding this document please email the Director, Trusted Digital Identity Framework at mailto:identity@dta.gov.au.

Document Management

This document has been reviewed and endorsed by the following groups.

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Jan 2018
Commonwealth GovPass Design Authority	Feb 2018

Change log

Version	Date	Author	Description of the changes
0.01	May 2017	SJP	Initial version
0.02	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 Trust Framework documents.
0.03	Sept 2017	SJP	Minor updates to support the public consultation draft.
0.04	Jan 2018	SJP	Incorporates feedback from stakeholders and public consultation.
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority

Conventions

The following conventions[1] are used in this document.

- **MUST** – means an absolute requirement of this document.
- **SHOULD** – means there may exist valid reasons to ignore a particular item in this document, but the full implications need to be understood before choosing a different course.

[1] These conventions are taken from Request for Comments 2119 (RFC2119) – Keywords for use in RFCs to indicate requirements levels

Contents

1 Introduction

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity ‘eco-system’ (the ‘identity federation’). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document should be read in conjunction with the *Trust Framework: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

This document defines the requirements to be met by government agencies and organisations in order to achieve TDIF accreditation for their identity service[2]. This document does not define maximum periods in which individual activities or the accreditation process are to take, as this is largely driven by the Applicant.

Applicants **SHOULD** be able to complete the Trust Framework Accreditation Process within 12 months of starting the process. 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 address any non-compliance issues to the satisfaction of the Trust Framework Accreditation Authority.

Although Applicants **SHOULD** have a fully operational identity service prior to undergoing accreditation, the Trust Framework Accreditation Process does support Applicants that develop their identity service over the course of their accreditation. Applicants that operate mature identity services who are familiar with the Trust Framework requirements are likely to complete the Trust Framework Accreditation

[2] See the *Trust Framework: Annual Review* for ongoing accreditation requirements.

Process much quicker than an Applicant who is either unfamiliar with the process or is still developing their identity service.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Authorised Assessors.
- Relying Parties.
- Trust Framework Accreditation Authority.

2 Accreditation roles and responsibilities

2.1 Applicant

Applicants that apply for Trust Framework accreditation for their identity service will undergo rigorous evaluations. This includes compliance with requirements for identity proofing, authentication credential management, privacy, protective security, accessibility, usability, risk management, fraud control, technical integration and service operations.

The Applicant is responsible for:

- Formally advising the Trust Framework Accreditation Authority of its intention to undergo the Trust Framework Accreditation Process.
- Preparing all required documentation within agreed timeframes with the Trust Framework Accreditation Authority.
- Obtaining the required independent assessments from Authorised Assessors.
- Remediating all identified non-conformance and adverse findings to the satisfaction of the Trust Framework Accreditation Authority.
- Formally advising the Trust Framework Accreditation Authority of its intention to leave the program in the event it:
    - No longer wants to undergo the Trust Framework Accreditation Process.
    - Can no longer comply with Trust Framework requirements once accredited.
    - Chooses no longer to do so.

Upon completion of the Trust Framework Accreditation Process, the Applicant and the Trust Framework Accreditation Authority will sign an accreditation agreement. This sets out the respective rights and obligations of the Trust Framework Accreditation Authority and the Applicant (now Accredited Provider) for the provision of its identity services. This agreement will specify arrangements in relation to:

- Maintenance of accreditation - what actions the Accredited Provider **MUST** take in order to maintain accreditation from year to year.
- Dispute settlement, including appeal mechanisms.
- Management of security and privacy breaches.

The Accredited Provider **MUST** be able to demonstrate through an annual compliance audit[3] that it continues to offer an identity service in a manner consistent with the documents and evaluations that formed the basis of its accreditation.

2.2 Trust Framework Accreditation Authority

The Trust Framework Accreditation Authority is responsible for:

- Ensuring that the Trust Framework Accreditation Process is conducted with due care and in accordance with the published Trust Framework documents.
- Reviewing, within agreed timeframes, all relevant Applicant documentation to ensure conformance to the published Trust Framework documents.
- Considering all reports and recommendations from Authorised Assessors.
- All decisions in relation to the accreditation of Applicants and ongoing accreditation of Accredited Providers, including decisions to accept a non-conformance against the Trust Framework requirements where it considers evidence provided by the Applicant is sufficient in favour of non-conformance.
- The Trust Framework Accreditation Authority interprets conformance against Trust Framework requirements as either:
    - Demonstrating compliance against Trust Framework requirements.
    - In a protective security context, the Trust Framework Accreditation Authority accepting a waiver for the use of alternative controls. See the *Trust Framework: Protective Security Requirements* for further information on waivers.

2.3 Authorised Assessors

Authorised 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 Trust Framework.

Authorised Assessors are responsible for:

[3] See the *Trust Framework: Annual Review* for ongoing accreditation requirements.

- Assessing the Applicant’s compliance against particular Trust Framework requirements.
- Documenting their findings, which:
    - Summarise the activities performed during the evaluation.
    - Suggest remediation actions to address areas of non-compliance or unmitigated risk.
    - Recommend whether or not the Applicant has satisfied specific requirements of the Trust Framework.
- Providing their findings to the Trust Framework Accreditation Authority.

The ‘*Trust Framework Accreditation Process’* section of this document outlines when an Applicant is required to use an Authorised Assessor. Specifically, Applicants **MUST** use Authorised Assessors for the following activities:

- Privacy[4]:
    - Privacy Impact Assessment (PIA).
    - Privacy audit.
- Protective security[5]:
    - Information Security Registered Assessors Program (IRAP).
    - Information security penetration testing.
- Usability and accessibility[6]:
    - Usability and accessibility testing.

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

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

[6] See *Trust Framework: Accessibility and Usability Requirements* for further information.

3 Trust Framework Accreditation Process

3.1 Overview

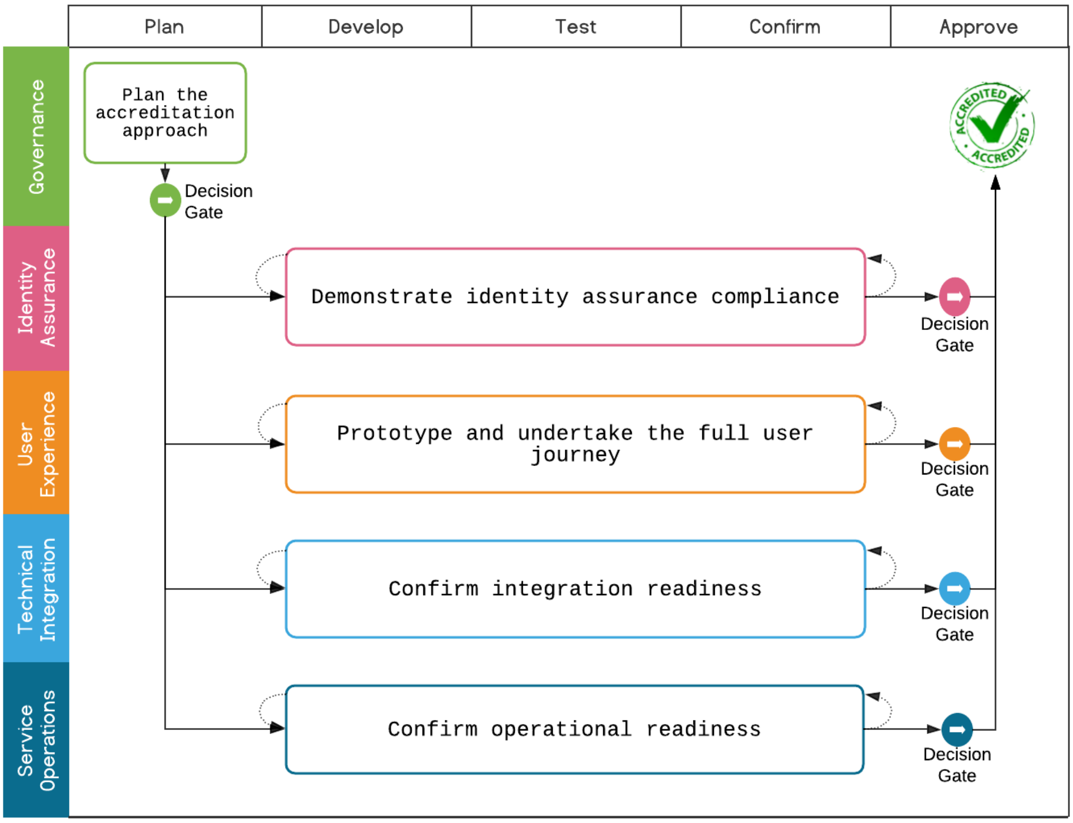
The Trust Framework Accreditation Process includes a number of accreditation activities and involves a combination of documentation, independent evaluations and operational testing that the Applicant **MUST** complete to the satisfaction of the Trust Framework Accreditation Authority in order to achieve accreditation. These activities are linked by a series of work streams that cover governance, identity assurance, user experience, technical interoperability and service operations. Figure 1 below provides an overview of the Trust Framework Accreditation Process.

Progress through the accreditation process is managed by a series of decision gates. The decision gates are used by the Trust Framework Accreditation Authority to evaluate the Applicant's progress towards accreditation. Arrows show the relationships between accreditation activities. The activities in all workstreams can be iterated. This approach supports Applicants that are still developing their identity service who don't meet all the requirements of a particular workstream and are not yet ready to pass a decision gate.

Assuming approval has been granted by the Trust Framework Accreditation Authority to progress beyond the '*plan the accreditation approach*' activity, the Applicant is free to choose which activity they complete next. For example, the Applicant can choose to complete all accreditation activities within a particular workstream, or complete one activity in a workstream then switch to another workstream.

Applicants can apply to undergo the Trust Framework Accreditation Process for fully operational, production-ready or in-development identity services, however, the Trust Framework Accreditation Authority will only grant accreditation to fully operational identity services that have successfully passed all decision gates. The Trust Framework Accreditation Authority **will not** grant provisional accreditations.

Figure 1: Trust Framework Accreditation Process

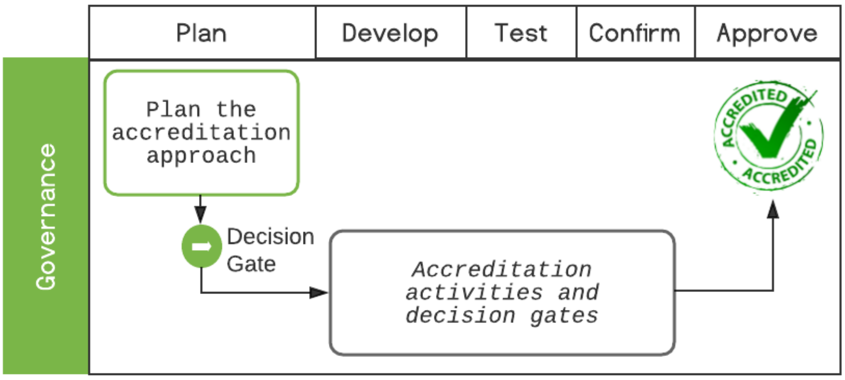


All costs associated with accreditation are to be met by the Applicant. Although the DTA does not charge Applicants a fee to complete the accreditation process, it will cost the Applicant money to complete certain accreditation criteria; for example, the PIA and IRAP. Depending on the complexity and timeliness of the evaluation to be performed, the cost to the Applicant could be more than expected. Applicants **SHOULD** contact several Authorised Assessors to get a sense of the cost, duration and complexity of an assessment prior to engaging a particular Authorised Assessor. The Applicant **SHOULD** also understand the requirements, compliance obligations and likely costs associated with pursuing accreditation before commencing the Trust Framework Accreditation Process.

3.2 Governance workstream

This workstream defines the requirements to be met by the Applicant in order to achieve Trust Framework accreditation.

Figure 2: Governance workstream


Plan
Develop
Test
Confirm
Approve
Governance
Plan the accreditation approach
Decision Gate
Accreditation activities and decision gates
ACCREDITED
ACCREDITED

3.2.1 Plan the accreditation approach

The Applicant **MUST**:

- Formally advise the Trust Framework Accreditation Authority of the intention to undergo the Trust Framework Accreditation Process.
    - This includes providing the Trust Framework Accreditation Authority with any relevant waivers against ISM or PSPF controls. As per the *Trust Framework: Protective Security Requirements*, the Trust Framework Accreditation Authority will either accept or reject the waiver for the purpose of Trust Framework accreditation. If the waiver is rejected the Applicant **MUST** implement the protective security control as defined in the *Trust Framework: Protective Security Requirements*.
- Supply a completed Accreditation Plan to the Trust Framework Accreditation Authority, which outlines the approach to be taken by the Applicant to complete each accreditation activity and pass each decision gate.

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 to the Trust Framework Accreditation Authority that it has satisfied each accreditation activity. This includes key dates, milestones and the proposed date by which Trust Framework accreditation will be achieved.
- A description of how the Applicant will resolve adverse findings at decision gates.

The Trust Framework Accreditation Authority **MUST**:

- Ensure the applicable Trust Framework documents (listed in Annex A) are available to the Applicant in a timely manner.
- Formally acknowledge the Applicant's intention to undergo accreditation.
- Advise the Applicant of its decision to either accept or reject the provided waivers.

3.2.2 Governance decision gate

The Trust Framework Accreditation Authority **MUST** advise the Applicant whether the Accreditation Plan is sufficiently detailed to progress beyond the Governance decision gate.

- If the Accreditation Plan is sufficiently detailed, the Trust Framework 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 Trust Framework 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.

3.2.3 Accreditation granted

The Applicant's identity service will be connected to the live implementation of the Identity Exchange environment. A period of live operation will follow, where rapid fixes may be required by the Applicant to resolve issues not discovered in the previous accreditation activities.

The Applicant **MUST** sign two copies of the Memorandum of Agreement and return both copies to the Trust Framework Accreditation Authority.

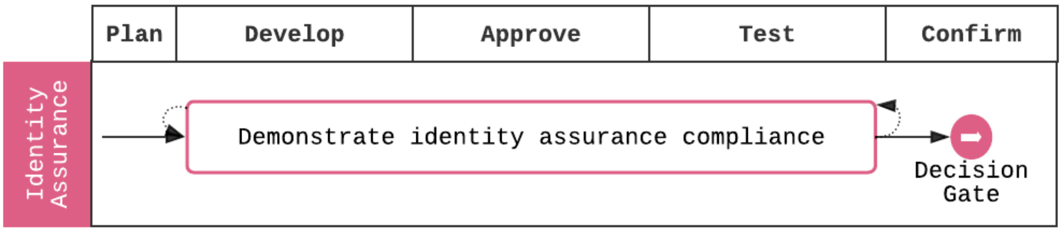
The Trust Framework Accreditation Authority **MUST**:

- advise the Applicant that its identity service has successfully been onboarded to the live implementation of the Identity Exchange environment.
- Counter-sign two copies of the Memorandum of Agreement and return one to the Applicant.

3.3 Identity Assurance workstream

This workstream defines the requirements to be met by the Applicant in order to pass the Identity Assurance decision gate.

Figure 3: Identity Assurance workstream



3.3.1 Demonstrate identity assurance compliance

The Applicant **MUST**:

- Demonstrate its identity service conforms to the applicable Trust Framework documents listed in Annex A.
- Undergo an independent PIA by an Authorised Assessor.
- Undergo an independent privacy audit by an Authorised Assessor.
- Undergo an independent IRAP Assessment by an Authorised Assessor.

- Undergo an independent information security penetration test by an Authorised Assessor.
- Remediate any non-compliances or adverse findings to the satisfaction of the Trust Framework Accreditation Authority.

The Trust Framework Accreditation Authority **MUST**:

- Conduct an expert review of the Applicant's identity assurance documentation.
- Advise the Applicant of areas of compliance and non-conformance against the applicable Trust Framework documents listed in Annex A.
    - The Trust Framework Accreditation Authority reserves the right to exclude any items in the applicable Trust Framework documents from consideration at its sole discretion.
    - The Trust Framework Accreditation Authority may choose to outsource the identity assurance documentation review to an independent expert.
- Advise the Applicant whether the proposed remediation actions are acceptable.
    - If the proposed remediation actions are acceptable the Trust Framework Accreditation Authority will advise the Applicant accordingly.
    - If the proposed remediation actions are not acceptable the Trust Framework Accreditation Authority will advise the Applicant accordingly, 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.

3.3.2 Identity Assurance decision gate

The Trust Framework Accreditation Authority **MUST** determine whether an Applicant has met all requirements of the Identity Assurance workstream.

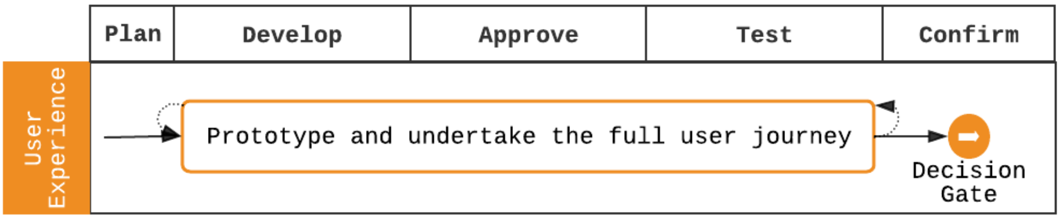
- The Applicant will be advised by the Trust Framework Accreditation Authority if it has met all requirements of the Identity Assurance workstream and its accreditation status will be updated accordingly.
- The Applicant will be advised by the Trust Framework Accreditation Authority if it has not met all requirements of the Identity Assurance workstream and has therefore has failed to pass the decision gate, the reasons why, and the

required actions to be taken by the Applicant in order for it to meet the requirements of the Identity Assurance workstream.

3.4 User Experience workstream

This workstream defines the requirements to be met by the Applicant in order to pass the User Experience decision gate.

Figure 4: User Experience workstream



3.4.1 Prototype and undertake the full user journey

The Applicant **MUST**:

- Prototype the user journey in accordance with the applicable Trust Framework documents listed in Annex A.
- Undergo an independent usability test or heuristic review of the journey by an Authorised Assessor.
- Make its user journey available for review by the Trust Framework Accreditation Authority.
- Respond to any requests made by the Trust Framework Accreditation Authority in relation to the usability of their identity service.
- Remediate any non-compliances or adverse findings to the satisfaction of the Trust Framework Accreditation Authority.

The Trust Framework Accreditation Authority **MUST**:

- Conduct a review of the user journey and associated evidence.
- Advise the Applicant of areas of compliance and non-conformance against the applicable Trust Framework documents listed in Annex A.

    - The Trust Framework Accreditation Authority reserves the right to exclude any items in the applicable Trust Framework documents from consideration at its sole discretion.
    - The Trust Framework Accreditation Authority may choose to outsource the review to an independent expert.
- Advise the Applicant whether the proposed remediation actions are acceptable.
    - If the proposed remediation actions are acceptable the Trust Framework Accreditation Authority will advise the Applicant accordingly.
    - If the proposed remediation actions are not acceptable the Trust Framework Accreditation Authority will advise the Applicant accordingly, 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.

3.4.2 User Experience decision gate

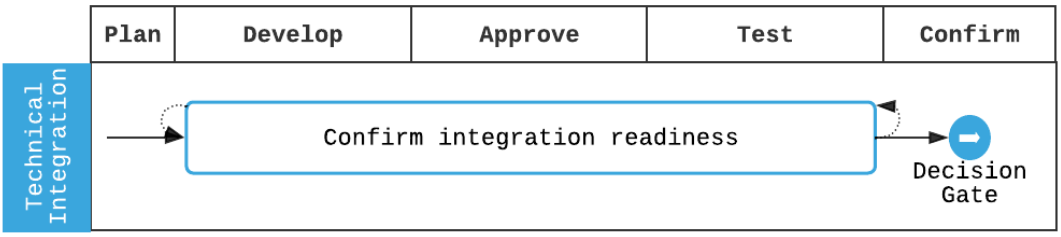
The Trust Framework Accreditation Authority **MUST** determine whether an Applicant has met all requirements of the User Experience workstream.

- The Applicant will be advised by the Trust Framework Accreditation Authority if it has met all requirements of the User Experience workstream and its accreditation status will be updated accordingly.
- The Applicant will be advised by the Trust Framework Accreditation Authority if it has not met all requirements of the User Experience workstream and has therefore has failed to pass the decision gate, the reasons why, and the required actions to be taken by the Applicant in order for it to meet the requirements of the User Experience workstream.

3.5 Technical Integration workstream

This workstream defines the requirements to be met by the Applicant in order to pass the Technical Integration decision gate.

Figure 5: Technical Integration workstream



3.5.1 Confirm integration readiness

The Applicant **MUST**:

- Ensure the integration readiness of its identity service conforms to the applicable Trust Framework documents listed in Annex A.
- Provide documented evidence to the Trust Framework Accreditation Authority of their Technical Integration readiness and responsible points of contact in their organisation.
- Respond to any requests made by the Trust Framework Accreditation Authority in relation to the Technical Integration readiness for their identity service.
- Demonstrate that all test use cases defined within their Technical Integration documentation and test plans have been successful.
- Remediate any adverse findings to integration tests to the satisfaction of the Trust Framework Accreditation Authority.

The Trust Framework Accreditation Authority **MUST**:

- Conduct an expert review of the Applicant's Technical Integration documentation.
- Evaluate the Applicant's Technical Integration test results.
- Advise the Applicant of areas of compliance and non-conformance against the applicable Trust Framework documents listed in Annex A.
  - The Trust Framework Accreditation Authority reserves the right to exclude any items in the applicable Trust Framework documents from consideration at its sole discretion.
  - The Trust Framework Accreditation Authority may choose to outsource the review to an independent expert.

- Advise the Applicant whether the proposed remediation actions are acceptable.
    - If the proposed remediation actions are acceptable the Trust Framework Accreditation Authority will advise the Applicant accordingly.
    - If the proposed remediation actions are not acceptable the Trust Framework Accreditation Authority will advise the Applicant accordingly, 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.

3.5.2 Technical Integration decision gate

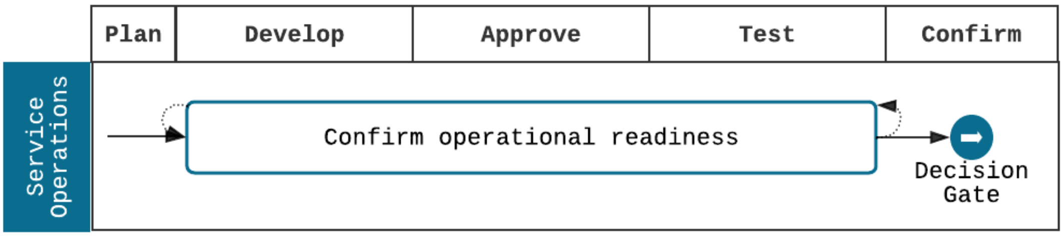
The Trust Framework Accreditation Authority **MUST** determine whether an Applicant has met all requirements of the Technical Integration workstream.

- The Applicant will be advised by the Trust Framework Accreditation Authority if it has met all requirements of the Technical Integration workstream and its accreditation status will be updated accordingly.
- The Applicant will be advised by the Trust Framework Accreditation Authority if it has not met all requirements of the Technical Integration workstream and has therefore has failed to pass the decision gate, the reasons why, and the required actions to be taken by the Applicant in order for it to meet the requirements of the Technical Integration workstream.

3.6 Service Operations workstream

This workstream defines the requirements to be met by the Applicant in order to pass the Service Operations decision gate.

Figure 6: Service Operations workstream



3.6.1 Confirm operational readiness

The Applicant **MUST**:

- Ensure the service operations aspects of its identity service conforms to the applicable Trust Framework documents listed in Annex A.
- Provide documented evidence to the Trust Framework Accreditation Authority of their service operations and responsible points of contact in their organisation.
- Undertake a series of collaborative tests with the Trust Framework Accreditation Authority to ensure operational readiness of the end-to-end service.
- Demonstrate that all scenarios defined within their service operations documentation have been successfully tested.
- Respond to any requests made by the Trust Framework Accreditation Authority in relation to the service operations for their identity service.
- Remediate any adverse findings to service operations readiness to the satisfaction of the Trust Framework Accreditation Authority.

The Trust Framework Accreditation Authority **MUST**:

- Conduct an expert review of the Applicant's service operations documentation.
- Evaluate the Applicant's operational readiness test results.
- Advise the Applicant of areas of compliance and non-conformance against the applicable Trust Framework documents listed in Annex A.
    - The Trust Framework Accreditation Authority reserves the right to exclude any items in the applicable Trust Framework documents from consideration at its sole discretion.

    - The Trust Framework Accreditation Authority may choose to outsource the review to an independent expert.
- Advise the Applicant whether the proposed remediation actions are acceptable.
    - If the proposed remediation actions are acceptable the Trust Framework Accreditation Authority will advise the Applicant accordingly.
    - If the proposed remediation actions are not acceptable the Trust Framework Accreditation Authority will advise the Applicant accordingly, 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.

3.6.2 Service Operations decision gate

The Trust Framework Accreditation Authority **MUST** determine whether an Applicant has met all requirements of the Service Operations workstream.

- The Applicant will be advised by the Trust Framework Accreditation Authority if it has met all requirements of the Service Operations workstream and its accreditation status will be updated accordingly.
- The Applicant will be advised by the Trust Framework Accreditation Authority if it has not met all requirements of the Service Operations workstream and has therefore has failed to pass the decision gate, the reasons why, and the required actions to be taken by the Applicant in order for it to meet the requirements of the Service Operations workstream.

4 References

The following information sources have been used in developing this document.

1. Bradner, S. 1997, '*Key words for use in RFCs to Indicate Requirements Level' (Requests for Comment 2119)*, Internet Engineering Task Force, Switzerland. https://tools.ietf.org/html/rfc2119

Annex A: Applicable Trust Framework documents

The table below indicates the applicable Trust Framework documents for each workstream of the Trust Framework Accreditation Process.

Table 1: applicable Trust Framework documents

Document / Workstream	Governance	Identity Assurance	User Experience	Technical Integration	Service Operations
Overview and Glossary	X				
Accreditation Process	X				
Privacy Requirements	X	X		X	X
Protective Security Requirements	X	X		X	X
Risk Management Requirements	X	X		X	X
Fraud Control Requirements	X	X		X	X
Identity Proofing Requirements	X	X			
Authentication Credential Requirements	X	X			
Usability and Accessibility Requirements	X	X			
Technical Integration Requirements	X		X		
SAML 2.0 Profile	X			X	
OpenID Connect Profile	X			X	
Service Operations Requirements	X			X	
Memorandum of Agreement	X				X