Australian Government
Digital Transformation Agency

Fraud Control Requirements

Trusted Digital Identity Framework
August 2018, version 1.2

dta

Digital Transformation Agency

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

The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" 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 have difficulties accessing this document, or have questions or comments regarding this document please email the Director, Trusted Digital Identity Framework at identity@dta.gov.au.

Document Management

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

Change log

Version	Date	Author	Description of the changes
0.01	Sept 2017	PH	Initial version
0.02	Jan 2018	PH	Feedback incorporated from public consultation
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority
1.1	Mar 2018	PH	Restructured and feedback incorporated. Training requirements grouped together. Annex B added.
1.2	Aug 2018	PH	Stakeholder feedback incorporated

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 *TDIF: 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 lists the TDIF Fraud Control Requirements (FCRs) which are applicable to an Applicant's identity service being accredited against the TDIF, but not its broader organisational or agency activity. For example, the FCRs apply to an organisation or agency's identity service if it is accredited as an Identity Service Provider but it does not apply to the other functions such HR, finance, or other business services.

The intended audience for this document includes:

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

For the purpose of this document, both Applicants who wish to become accredited under the TDIF and Accredited Providers are referred to as "Applicants".

2 Fraud control requirements

2.1 Fraud control responsibilities

2.1.1 Governance

Applicants **MUST** establish and maintain systems for managing the risk and incidents of fraud for all identity services accredited under the TDIF.

Applicants **MUST** take all reasonable measures to prevent, detect and deal with fraud relating to their identity service, by:

- Conducting fraud risk assessments regularly and when there is a substantial change in the structure, functions or activities of the identity service.
- Developing and implementing a Fraud Control Plan that deals with the identified risks as soon as practicable after conducting a risk assessment.
- Having appropriate mechanisms for preventing fraud, including by ensuring that the Applicant's personnel are made aware of what constitutes fraud and the risk of fraud is taken into account in the planning and operation of the Applicant's identity service.
- Having an appropriate mechanism for detecting incidents of fraud or suspected fraud, including a process for the Applicant's personnel and individuals who use the Applicant's identity service to report suspected fraud confidentially.
- Having an appropriate mechanism for investigating and otherwise dealing with incidents of fraud or suspected fraud.
- Having an appropriate mechanism for recording and reporting incidents of fraud or suspected fraud.

Applicants that are IdPs **MUST** ensure consent is collected from the individual before their identity information is disclosed to a Relying Party. Depending on the transmission path, consent **MAY** be collected by an intermediary (e.g. an Identity Exchange). If no intermediary is used then consent **MUST** be collected by the IdP prior to disclosure.

A list of fraud control responsibilities can be found at Annex A of this document.

2.1.2 Fraud Risk Assessment

Applicants **MUST** conduct Fraud Risk Assessments for each TDIF accredited service:

- Prior to systems being deployed into operation,
- Annually.
- When there is a substantial change in their structure, functions or activities.
- When a new fraud risk is identified.
- When there are significant changes in technological capabilities which impacts on the service or services provided.
  e.g. If the IdP implements its own face to passport chip matching technology in preference to using the Facial Verification Service, a review of the risk assessment would be required.

Applicants **MUST** demonstrate in their Fraud Risk Assessments, that they have considered, mitigated, and/or managed identified fraud risks.

Further information on risks that **MUST** be considered are listed in the *TDIF: Risk Management Requirements* at *Annex A: Potential Sources of Risk*.

2.1.3 Fraud Control Plan

Applicants **MUST** develop a Fraud Control Plan for each identity service accredited under the TDIF.

The Fraud Control Plan **MUST** that clearly delineates between process, architecture and technology-based risks while undertaking their risk assessment and cover:

- Fraud risks arising due to internal process: Risks arising due to processes conducted by Personnel. E.g. if counter personnel who are not trained to and do not demonstrate competency in face matching are required to do in-person face matching.
- Fraud risks arising due to architecture: a risk arising due to the way information is stored, shared or interpreted. E.g. a credential is not verified with the credential issuer to determine if a credential with those details was issued.
- Fraud risks arising due to technological capabilities, issues or gaps. E.g. biometric face verification where no liveness detection is done when the image is being captured.

The Fraud Control Plan **MUST** include, at a minimum:

- Staff access control and auditing processes.

- Responsibilities for managing different levels of fraud.
- Fraud victim support processes.

The Applicant **MUST** add new fraud risks and their associated management strategies to their Risk Management Plan in accordance with their risk management process. Fraud Control Procedures

Fraud Control Procedures provide personnel with guidance to minimise fraud in the workplace and manage it should it occur. They are a separate document to the Risk Management Plan.

The Fraud Control Procedures **MUST:**

- Be based on the Fraud Risk Assessment and the Fraud Management Plan.
- Updated as new types of fraud and fraud controls are identified.

At a minimum, the Fraud Control Procedures **MUST** identify the following:

- The definition and description of fraud within the Applicant's identity service.
- Roles and responsibilities for fraud control for the Applicant's identity service.
- A description of fraud mitigation practices.
- Risk and scenario-based fraud control procedures.
- Points of contact when fraud or potential fraud have been identified.
- Instructions for victim support.

2.2 Fraud prevention

Applicants **MUST** have in place a series of reasonable, evidence-based measures to prevent fraud. A list of fraud prevention objectives can be found at Annex B.

Applicants **MUST**:

- Have in place auditable processes and technologies that prevent or significantly reduce fraud from occurring.
  E.g. IdP enrolment processes flows that prevent an individual from committing identity fraud with an IdP using a stolen identity document. If a person wants to sign up for a digital identity at IP2 or above, they would require multiple verifiable identity documents or credentials. It becomes harder to commit fraud with every

additional verifiable document or credential with the same or demonstrably linked identity attributes.

- Conduct background checks prior to commencement, on personnel with access to personal information to ensure that they do not have a history of misconduct and do not have ties to organised crime.
- Conduct regular audits of personnel activities relating to accessing, managing or disclosing personal information.
- Ensure centralised logging is implemented and sufficient event correlation is available to identify anomalous activity.
- Educate individuals on current identity-related threats (e.g. social engineering) and the appropriate and inappropriate uses of their digital identity and authentication credentials.

2.2.1 Monitoring requirements

Applicants **MUST:**

- Where permissible, use fraud information gathered (through fraud incidents, investigations and reports) to enhance fraud control capabilities.
- Use fraud monitoring tools and analytics set up and monitored by experienced data analysts, to develop fraud profiles and if possible predict instances of fraud.
- Perform ongoing real time monitoring and audits of systems and processes.
- Assess the effectiveness of monitoring and tools and make changes based on these assessments.

Where personal information has been compromised as a result of access by personnel or third-party providers, the Applicant **MUST** investigate and take appropriate action against personnel and third party involved.

2.2.2 Personnel training requirements

Applicants **MUST** deliver targeted and relevant fraud control training to all personnel including:

- What constitutes fraud within the Applicant's identity service.
- Fraud risk management roles and responsibilities.
- Procedures for following up and referring suspected fraud.

- Procedures for reporting when fraud is detected.

Fraud control training **MUST**:

- Reflect the Fraud Control Procedures, assisting personnel to prevent, detect and deal with fraud and describing roles and responsibilities within the Applicant's identity service.
- Be updated and made available to personnel as new procedures are implemented.
- Be refreshed annually.
- be summarised in a Fraud Control Procedures in straightforward and easy to understand formats.

Personnel **MUST**:

- Demonstrate understanding of this training prior to commencing work on the Applicant's identity service or having access to personal information.
- Be able to define identity fraud and demonstrate understand of the role of the Applicant service in reducing and managing fraud prior to commencing their roles.

Personnel primarily engaged in fraud control activities **MUST** possess or attain relevant competencies, qualifications or training to effectively carry out their duties.

Fraud control training **MAY**:

- be delivered in a number of ways including online and classroom learning.

2.2.3 Specialised training

2.2.3.1 Facial Recognition Training

Personnel responsible for making binding decisions (facial verification to link an individual to their document without the assistance of a biometric system) providing face to face services online or over the counter **MUST** demonstrate proficiency in facial recognition and face matching. Studies have shown that 1 in 10 people are capable of facial recognition of unknown faces (i.e. faces that they have not seen before) and of doing face matching of unfamiliar faces. It is therefore important that

Applicants only employ personnel who have demonstrated aptitude or competency in this field, to make binding decisions.

Applicants **MUST** ensure that all personnel undertaking facial recognition and matching tasks have demonstrated competency in and aptitude for facial recognition and facial comparison.

2.2.3.2 Fraud Investigations Training

Applicants **MUST** ensure personnel responsible for undertaking fraud investigations are appropriately trained and have demonstrated competency in fraud investigation.

2.2.4 Awareness information for individuals

Applicants **MUST** provide information to individuals on how to safeguard their identity. Where scams are detected, Applicants **MUST** provide advice to individuals on how to avoid being scammed. Applicants **MAY** choose hire a specialised or accredited third party assist in this activity.

Applicants **SHOULD** make this information available to individuals in a number of formats e.g. instructional videos, online training, in-person walk-through and/or fact sheets.

2.3 Fraud detection

Fraud may be detected at a number of points throughout the identity life-cycle. Fraud may be detected and reported by the greatest opportunities to detect fraud arise:

- During the initial enrolment of an individual with an Identity Service Provider (IdP) and/or Credential Service Provider (CSP).
- By an Identity Exchange or Attribute Provider.
- During authentications or transactions.
- Through reporting by Relying Parties and individuals.

Applicants **MUST** undertake fraud monitoring activities based on available data, which **MUST** be analysed by members of staff with competency in using diagnostic tools and sufficient understanding and knowledge of the system in order to identify unusual behaviour.

Where Applicants become aware of specific types of fraud such as compromised batches of documents or identities, they **SHOULD** engage in rules-based fraud prevention – e.g. if advice is received by the applicant from an issuing agency or a reliable source, that certain batches of documents cannot be trusted or used, both the system and personnel **SHOULD** take this into account before enabling prospective individuals holding such documents to enrol.

Based on the assessed risk associated with a transaction, a Relying Party **MAY** request that aspects of an identity are re-proofed when an individual attempts to gain access to a service, this re-proofing might involve a request that the binding process is repeated at the time of the transaction. Re-proofing rules and processes **MUST** be documented in agreements for Relying Parties under the TDIF Operating Rules.

Where fraud or suspected fraud is reported to the Applicant or detected by the Applicant, the Applicant **MUST** assess the incident and ensure that appropriate stakeholders are notified as soon as possible. E.g. if an individual reports that their identity has been used without the knowledge or permission, the Applicants **MUST** advise the Identity Exchange of the instances of inappropriate use of a digital identity so that the Identity Exchange can notify the relevant Relying Parties.

When an incident of fraud is confirmed, the Applicant **MUST** take the actions specified in the Fraud Control Plan and Fraud Control Procedures to manage the fraud.

Where a suspected fraud incident is detected by, or reported to an Applicant, it **MUST** be assessed, actioned and the appropriate stakeholders notified as soon as possible in accordance with the Applicants Fraud Control Plan and Fraud Control Procedures.

2.4 Fraud investigations

Applicants are responsible for investigating instances of fraud or suspected fraud against them including investigating disciplinary matters, unless the matter is referred to and accepted by the Australian Federal Police (AFP) or another law enforcement agency.

The AFP, Commonwealth Attorney General's Department (AGD) and state and territory jurisdiction governments provide guidance on the requirements for fraud investigations.

If criminal activity is identified in an investigation, Applicants **MUST,** where permissible, notify the affected parties, ensuring that no information is shared inappropriately.

Applicants **MUST**:

- Have in place appropriate mechanisms, procedures and for investigating or otherwise dealing with incidents of fraud or suspected fraud.
- Have in place investigation and referral processes and procedures.
- Resolve fraud matters in accordance with relevant internal and external requirements where a law enforcement agency has declined a referral.
- Document decision criteria at critical stages in managing a suspected fraud incident.
- Resolve fraud investigations when they occur and advise stakeholders (particularly affected individuals, and where possible, identity federation participants) of the investigation outcome.
- Appropriately document decisions to use civil, administrative or disciplinary procedures, or to take no further action in response to a suspected fraud incident.

Law enforcement agencies may not always have the capacity to investigate fraud. Where a law enforcement agency has declined a referral, the Applicant **MUST** undertake the investigation and bring the investigation to a conclusion within a reasonable timeframe. It is acceptable for the Applicant to outsource the investigative function to a reasonable and reliable Australian-based third party capable of dealing with fraud matters.

2.4.1 Fraud investigation and monitoring tools

The Applicant **MUST** have in place systems or mechanisms in which potential fraud can be flagged and decision criteria are recorded and workflow and allocations of work are visible. E.g. A case management system for suspected fraud and fraud investigations.

This system will need to be capable of inputting information in accordance with the decision criteria in the Fraud Control Plan and the Fraud Control Procedures. This **SHOULD** include, but is not limited to criteria such as:

- When an incident is first identified.
- What type of fraud has been identified.
- The impacts on the identity.
- Frequency of use of the identity, location it was used etc.
- The outcome of the investigation.

The system will be used to appropriately document decisions to use civil, administrative or disciplinary procedures or to take no further action in response to a suspected or confirmed fraud incident.

2.5 Reporting fraudulent or potentially fraudulent activity

Where fraud is found to have occurred, Applicants **MUST**:

- Have appropriate mechanisms within their records to flag incidents of fraud and a repository or database for recording and reporting identities or credentials of concern against which all new individual registrations are matched.
- Conduct fraud reporting as required in annual compliance audits.

2.5.1 Information sharing

Where fraudulent or criminal activity is detected and where permissible, the Applicant **MUST** share this information with other TDIF participants.

Where a legitimate identity has been compromised and a victim was able to demonstrate ownership of the identity, the victim and all other parties notified by the Applicant **MUST** be advised of the outcome of the investigation.

Where an investigation discloses potential criminal activity involving another entity's activities or programs, Applicants **MUST** report the matter to that entity or agencies managing fraud on the behalf of that entity to the extent possible subject to relevant requirements of any Australian law.

Where a data breach as described in the *TDIF: Privacy Requirements* occurs, the Applicant **MUST** notify all data owners impacted, of the potential that their data may be used to commit fraud and assist potential victims to secure their digital identities and credentials.

2.6 Fraud victim support

Applicants **MUST**:

- Have in place processes and support services to assist individuals whose identities or authentication credentials have been compromised to manage the impact of the compromise.
- Enable victims to advise the Applicant when they become aware of any fraudulent activities using their identity.
- Prevent continued fraudulent use of an individual's accounts when fraud has been reported or where it appears highly likely that fraudulent activity is occurring based on available information.
- Where the Applicant identifies likely fraudulent activity, verify with the potential victim whether those activities are fraudulent.
- Where possible, advise parties within the identity federation of compromised or fraudulent identities.
- Ensure that identity attributes such as facial image are re-proofed when a fraud victim is identified.

2.6.1 Communications channels for fraud victims

The Applicant **MUST** have in place processes such as appropriate identification of an individual whose identity has been compromised and appropriate technologies to enable the Applicant to flag the identity as compromised.

The Applicant **MUST** have sufficient qualified personnel managing communications channels (e.g. online, face-to-face and telephone) to provide victim support services within a reasonable timeframe. A third-party service provider may be able to provide this type of assistance.

Personnel providing support over the telephone or face to face **MUST** be based in Australia and that the Applicant **MUST** have mechanisms in place to prevent client information from being inappropriately shared or used by third party providers.

2.6.2 Managing the identities of fraud victims

When a victim of fraud is identified or self-identifies, their identity **MUST** be re-proofed to the highest IP level[1] which they have met.

- There is no stipulation for IP 1 and IP 2.
- For IP 3 and IP 4 this **MUST** be done using the face-to-face channel.

Where the fraud victim's identity documents have been compromised, the victim should where possible, be able to use other documents to verify their identity or request that their digital identity is re-proofed using the binding step whenever the identity is used until the issue is resolved.

Where a fraud victim's identity has been compromised, the Applicant **SHOULD** supply evidence of the compromised identity to the victim, to assist in the management of their identity going forward. This evidence **SHOULD** include where possible:

- Their full name, date of birth and address (if known).
- The date of identity compromise occurred (if known).
- How the compromise occurred (if known).

The Applicant **MUST** assist the victim to investigate when the fraud commenced and advise Relying Parties through the Identity Exchange, of suspected fraudulent transactions.

Where the quality of a claim that an identity is fraudulent has been checked and Applicants are authorised by legislation or where there is consent from the victim, Applicants **MUST** advise other TDIF participants of any compromised or fraudulent identities they encounter.

The Applicant **SHOULD** provide the victim with a list of transactions that occurred for the period during which their identity was compromised.

[1] See the *TDIF: Identity Proofing Requirements* for further information on IP levels

2.6.3 Management of unusual account transactions

Applicants **MUST** verify with individuals that their identity account remains under their control when unusual transactions are detected, e.g. new device in different geolocation is used to access the account.

3 References

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

1. Attorney-General's Department, Commonwealth Fraud Control Framework, 2017, https://www.ag.gov.au/CrimeAndCorruption/FraudControl/Pages/FraudControlFramework.aspx
2. Australian Government Investigations Standards
3. Australian Signals Directorate, 2017, '2017 Australian Government Information Security Manual: Controls (ISM)', Australian Government, Canberra. https://www.asd.gov.au/infosec/ism/
4. Crimes Act 1914 (Cwth)
5. Criminal Code 1995 (Cwth)
6. Department of Finance, 2014, 'Commonwealth Risk Management Policy', Australian Government, Canberra. http://www.finance.gov.au/comcover/risk-management/the-commonwealth-risk-management-policy/
7. Public Governance, Performance and Accountability Act 2013 (Cwth)
8. Public Governance, Performance and Accountability Rule 2014 (Cwth)
9. Proceeds of Crime Act 2002 and the Proceeds of Crime Regulations 2002 (Cwth)
10. Public Service Act 1999 (Cwth)

Annex A – fraud control responsibilities

The table below identifies the responsibilities of Applicants accredited against the TDIF. The Trust Framework Accreditation Process applies to the first two categories listed in the table below and the TDIF Operating Rules apply to the latter two categories.

Table 2: Role-based fraud control responsibilities

Role	Responsibility
IdPs, CSPs, Attribute Providers	• Develops Fraud Risk Assessment and Fraud Control Plan. • Collects, verifies and stores appropriate personal information. • Educates individuals on how to safeguard their identity information within the IdP. • Ensures that information collected is accurate and up to date. • Issues digital identities and/or authentication credentials. • When authorised by an individual, enables verification of digital identity with Relying Party. • Provides fraud reporting channels to individuals, Relying Parties and law enforcement agencies as described in the Fraud Control Plan and the Fraud Control Procedures. • Advises the Identity Exchange of fraud-related transactions within the IdP. • Investigates reports of identity fraud within its user cohort. • Maintains records of identity fraud within its user cohort. • Assists victims of digital identity theft to regain control of their digital identity.
Identity Exchange	• Develops Fraud Risk Assessment and Fraud Control Plan. • Ensures the privacy of the individual when operating in the identity federation is maintained. • Advises IdPs, CSPs and Attribute Providers of fraud-related transactions reported by the Relying Party. • Advises Relying party of fraud-related transactions reported by the IdP, CSPs and Attribute Providers.
Relying Party	• Verifies identity information using services provided by the Accredited Provider. • Ensures where necessary through their own means of information collection, that enrolling individuals is unique in the context of their service. • Collects an individual's personal information to determine eligibility for their service. • Detects and report identity fraud and credential fraud-related transactions to the Identity Exchange.
Individuals	• Provides accurate identity information. • Corrects or update identity information with Document Issuers as identity information such as name changes. • Does not share account or identity information with third parties.

Role	Responsibility
	• Reports unauthorised use of their digital identity or authentication credential to both the Accredited Provider and the Relying Party as soon as they become aware of it.

Annex B – fraud control objectives

Table 3: fraud control objectives

Objective	Description	Requirements
Unique in context	Confirming that an individual can be distinguished from others in the intended context.	Applicants **MUST** ensure that there are no duplicate records and that documents issued to a single holder are not used by more than one identity.
Legitimate	Confirming with Authoritative Sources that the claimed identity has been legitimately created in Australia, either through birth or immigration.	Where possible, Applicants **MUST** verify credential details with an Authoritative Source or the Credential Issuer.
Operational	Verifying with authoritative or reliable sources that a claimed identity exists and has been in use in the Australian Community over time.	Applicants **MUST** conduct a Use in the Community check OR a Community Footprint Check.
Bound	Anchoring an individual to a claimed identity through biometric verification to an authoritative source.	For IP3 and above the matching of a user to the image on their Photo ID **MUST** occur, OR for CLs, checking that the credential was issued to the user through an authentication process.
Linked	Confirming that, where biographical attributes have changed, the new attributes relate to the same individual.	Where biographical identity attributes don't match e.g. due to change of name or date of birth, the Applicant **MUST** ensure that the changed attribute is linked to the previous attribute through a Commencement of Identity agency-issued linking document.
Not Fraudulent	Confirming that a claimed identity is neither fraudulent nor fictitious.	The Applicant checks whether the identity has been reported as stolen or appears on an internal list of known fraudulent identities and the Identity Exchange(s) conducts a check of its stolen and known fraudulent identities database.
Under the control of the User	Confirming that the User has access to or is in control of one or more selected contact channels.	validation check through a device check, an SMS or an email.