Australian Government

Digital Identity

04A Functional Guidance

Trusted Digital Identity Framework

Release 4.8 - Feb 2023

PUBLISHED VERSION

Department of Finance (Finance)

Licence

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 Providers*, 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

Finance 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 digitalid@finance.gov.au

Document management

Finance has reviewed and endorsed this document for release.

Change log

Document Version	Release Version	Date	Author	Description of the changes
0.1		Oct 2019	MC	Initial version
0.2		Dec 2019	MC	Updated to incorporate feedback provided by stakeholders during the second round of collaboration on *TDIF* Release 4
0.3		Mar 2020	MC, AV	Updated to incorporate feedback provided during the third consultation round on *TDIF* Release 4
1.0	4.0	May 2020		Published version
1.1	4.3	Feb 2021	JK	CRID0004 – Biometrics guidance changes, major style, format, grammar and referencing changes. CRID0013 – Templates updated and now available on website
1.2	4.4	June 2021	JK, MS	CRID0009 – Added *Digital Identity* Risk Management guidance, additional privacy guidance
1.3	4.6	Mar 2022	JK, AV, MS	Update of guidance to align with Release 4.6 of the TDIF Requirements.
NA	4.7	June 2022		No changes to document
NA	4.8	Feb 2023		No changes to document

All changes made to the TDIF are published in the TDIF Change Log which is available at Trusted Digital Identity Framework (TDIF) | Digital Identity

Contents

Introduction

This document provides guidance to *Applicants* undergoing the *TDIF Accreditation Process* on how to meet the *TDIF 04 Functional Requirements.* This document includes guidance on the following requirements sections:

- Fraud Control
- Privacy
- Protective Security
- User Experience
- Technical Testing
- Functional Assessments.

The intended audience for this document includes:

- *Accredited Provider*s
- *Applicant*s
- *Assessor*s
- *Relying Parties*.

Disclaimer

The guidance information provided in this document is here to support an *Applicant's* accreditation effort. It does not replace an *Applicant's* obligations to meet the *TDIF* requirements.

If any conflicts exist between the *TDIF* guidance and requirements, the requirements take precedence.

Digital Identity Risk Management

The design of an *Applicant*'s *Identity System* must be informed by an assessment of the risks associated with the operation of their *Identity System*.

*Risk Assessment*s should follow a methodology consistent with one of the following:

- International Standards Organisation (ISO) 31000 Risk Management Guidelines (*ISO 31000:2018 Risk Management - Guidelines*),
- International Electrotechnical Commission (IEC) 31010 Risk Management Techniques (*IEC 31010:2019 Risk Management – Risk Management Techniques*), or
- Australia/New Zealand Standard AS/NZ ISO 31000 Risk Management – Guidelines (*AS/NZ ISO 31000:2018 Risk Management –Guidelines*).

Misuse of *Digital Identity information* and *credentials* are key enablers of a range of fraudulent activity. A *Digital Identity Risk Assessment* should be undertaken in the context of digital service delivery and may be a component of broader fraud, privacy and protective security *Risk Assessment*s. For *TDIF Applicants,* risk management activities are linked to the following requirements:

In ***TDIF 04 Functional Requirements***:

- **Section 2** sets out the requirements for *Applicants* to conduct a fraud *Risk Assessment*, implement a *Fraud Control Plan* and manage fraud-related risks.
- **Section 3.2** and **Section 3.3** sets out the requirements for *Applicants* to implement effective privacy governance, including requirements to establish privacy roles, implement *Privacy Management Plans*, *Privacy Policies* and undergo *Privacy Impact Assessments* to identify and minimise privacy related risks.
- **Section 4** sets out the requirements for *Applicant*s to conduct an assessment of *Cyber Security Risks,* implement a *System Security Plan* and manage *Cyber Security Risks*.

- **Section 7.4** sets out the requirements for the *Applicant* to assess and respond to any identified instances of risks, non-compliances or recommendations by an *Assessor* for each *Functional Assessment*.

- **Appendix A**: **Risk Ratings** sets out the required risk ratings to be assigned to any risks, recommendations or non-compliances identified by an *Assessor* during a *Functional Assessment*. *Applicant*s must be familiar with the consequences of each rating.

In ***TDIF 05 Role Requirements*:**

- For *Identity Service Providers*: **Section 3.3** sets out requirements for *Applicant*s that choose to implement alternative *Identity Proofing* processes to conduct a *Risk Assessment* on any risks associated with implementing that alternative *Identity Proofing* process.
- For *Identity Service Providers*: **Section 3.8** sets out requirements for *Applicant*s that use biometrics in their identity proofing processes to conduct *Risk Assessment*s and consider biometric specific risks in their *Fraud Control* and *System Security Plans*.
- For *Credential Service Providers*: certain sections of the *CSP* requirements contain different *Risk Assessment* requirements depending on the type of credential the *Applicant* supports.

Once accredited, *Applicant*s must also be aware of the requirements in *TDIF 07 Maintain Accreditation* that set out the obligations for *Accredited Providers* to review and update their various *Risk Assessment* materials.

Conducting a Risk Assessment

Appendix A: Potential Sources of Risk of this document provides a list of potential sources of *Digital Identity* risk that *Applicants* should consider when undergoing *Risk Assessment* and management activities.

*Risk Assessment*s should consider the impacts to the organisation itself, as well as the risks associated with the misuse of any resulting *Digital Identity information* or *credentials* in the broader community, where appropriate. This includes the impacts on:

- ***Individuals***: for example, an entitled *Individual* has difficulty accessing a government service because their *Digital Identity* or *credential* has been used previously by an unauthorised *User* to claim the service. This may also

include other financial, psychological or legal impacts associated with recovering a stolen *identity*.

- **Organisations**: for example, fraudulently obtained genuine *identity documents* are used to create fraudulent *digital identities* and *credentials,* which are used to commit fraud against businesses resulting in losses.

- **Government agencies**: for example, the incorrect attribution of *Digital Identity* to unauthorised *Users* resulting in significant losses for an agency, including increased risks of fraud-related crime against the agency or recipients of its benefits or services.

- **The broader Australian Identity landscape**: for instance, if the issuance of an *identity document* can be used in combination with other evidence types to fraudulently obtain higher-integrity *identity documents*. This type of fraudulent behaviour may result in impacts to *Individuals*, organisations, or government agencies.

The *Risk Assessment* should consider risk mitigation strategies that do not involve *identity proofing*. For example, some *Digital Identity* risks could be mitigated by supporting fraud detection processes (such as internal data cleansing, data matching against other organisation records or data analysis to detect suspicious transactions). However, these processes must also be considered in the context of an *Applicant's* obligations to meet the *TDIF* privacy, fraud and security requirements.

Organisations should review and refine their *Risk Assessment* strategies on an ongoing basis and continue to monitor and respond to emerging *identity*-related risks and vulnerabilities.

Fraud Control Guidance

The *TDIF* Fraud Control Requirements are based on the Australian Government Attorney-General's Department *Commonwealth Fraud Control Framework* (*CFCF*) and *Australian Government Investigation Standards* (*AGIS*).
While these policies and standards were developed for use by Australian Government entities, they contain useful guidance and information that may aid commercial and other jurisdiction government *Applicants* during their *TDIF accreditation*.

Applicants that undergo the *TDIF Accreditation Process* should note the following:

- Refences to 'agencies', '*accountable authority'*, 'Commonwealth entities', 'entities', 'officials' and 'Australian Government' in the *CFCF* or *AGIS* are to be interpreted as referring to the *Applicant*.

For *Applicants* who are required to comply with the below standards, to the extent of conflict between:

- Any requirement in these *TDIF* requirements and the current edition of the *CFCF*, then the *CFCF* takes precedence.
- Any requirement in these *TDIF* requirements and the current edition of the *AGIS*, then the *AGIS* takes precedence.
- The *AGIS* and law, then the legislative requirement will prevail.

Sources:
The Australian Government Attorney-General's Department *Commonwealth Fraud Control Framework* (*CFCF*) is available online. See:
https://www.ag.gov.au/integrity/publications/commonwealth-fraud-control-framework
The *Australian Government Investigation Standards* (*AGIS*) is available from the Attorney-General's Department. See:
https://www.ag.gov.au/integrity/publications/australian-government-investigations-standards-2011

Digital Identity Fraud Controller

*Relates to TDIF requirements **FRAUD-02-01-01** to **FRAUD-02-01-04** of **section 2.1** in the TDIF 04 Functional Requirements.*

For Australian Government, State and Territory entities, their Accountable Authority can fulfil the role of the *Digital Identity Fraud Controller.*

Part 4 of the *CFCF* includes guidance for *Applicants* on their responsibilities and accountability for fraud control arrangements.

The assessment of the *Digital Identity Fraud Risk* should analyse the latest industry information and threats, as well as the views of relevant stakeholders to ensure robust *Risk Assessment* practice. **Appendix A: Potential Sources of Risk** of this document provides a list of some potential sources of *Digital Identity* Fraud Risk that *Applicants* should consider when undergoing this assessment. See the ***Digital Identity* Risk Management** section of this document for further guidance in conducting this assessment.

Part 5 of the *CFCF* includes further guidance on conducting a *Risk Assessment*.

ISO 31000:2018 Risk Management - Guidelines provides further guidance in preparing, conducting and maintaining a *Risk Assessment*.

Digital Identity Fraud Control Plan

*Relates to TDIF requirements **FRAUD-02-02-01** to **FRAUD-02-02-02a** of **section 2.2** in the TDIF 04 Functional Requirements.*

Part 6 of the *CFCF* includes guidance for *Applicants* on *Fraud Control Plans*. It is expected that the *Risk Assessment* conducted by the *Applicant* under FRAUD-02-01-02 will inform the development of the *Fraud Control Plan*. Where the *Fraud Control Plan* is reviewed under FRAUD-02-02-02, the *Applicant* should consider whether this *Risk Assessment* also needs to be reviewed and updated.

A template for the Fraud Control Plan is available from the *Digital Identity* website. See: Trusted Digital Identity Framework (TDIF) | Digital Identity

Digital Identity Fraud Prevention, Awareness and Training

*Relates to TDIF requirements **FRAUD-02-03-01** to **FRAUD-02-03-03** of **section 2.3** in the TDIF 04 Functional Requirements.*

Part 7 of the *CFCF* includes guidance for *Applicants* on the implementation of fraud prevention, awareness, and training initiatives.

These initiatives involve:

- Prevention through controls
- Awareness raising initiatives
- Training for Fraud Control Officials
- Training for Fraud Control Officials (Investigators)

For *Applicants* who do not interact directly with *Users*, reasonable steps for providing advice about fraud risks and incidents may include steps taken to ensure that *Relying Parties* or other providers of identity who do interact with *Users* provide that advice. The intent is that the *Applicant* works to ensure this information is available to their *Users*, rather than placing the obligation on the *Applicant* to directly provide that information. When determining whether reasonable steps have been taken, *Finance* will consider:

- The likelihood of *Individual*s being able to access that advice
- The practicality of potential steps to be taken to advise *Individual*s of fraud risks and incidents
- The likely harm that might result if an *Individual* is not made aware of particular fraud risks and incidents, and what would be reasonable to prevent that harm eventuating.

Fraud Monitoring and Detection

*Relates to TDIF requirements **FRAUD-02-04-01** to **FRAUD-02-04-02b** of **section 2.4** in the TDIF 04 Functional Requirements.*

Part 9 of the *CFCF* includes guidance for *Applicants* on the detection, investigation, and response to fraud incidents.

Incident Management, Investigations and Reporting

*Relates to TDIF requirements **FRAUD-02-05-01** to **FRAUD-02-05-06a** of **section 2.5** in the TDIF 04 Functional Requirements.*

Part 9 and Part 11 of the *CFCF* includes guidance for *Applicants* on incident management, investigations, and reporting for fraud incidents.

The intent of these requirements is to ensure that an *Applicant* is investigating *Digital Identity Fraud Incidents* sufficiently to mitigate the adverse effects of the incident and minimise the risk of recurrence of similar incidents.

Where an *Applicant* is supporting another entity in conducting an investigation, reasonable steps would include the provision of any relevant information about an actual or suspected *Digital Identity Fraud Incident* to that entity.

The Australian Government Investigation Standards (AGIS) contains further guidance on conducting investigations. See: https://www.ag.gov.au/sites/default/files/2020-03/AGIS%202011.pdf.

Support for victims of *Digital Identity* fraud

*Relates to TDIF requirements **FRAUD-02-06-01** to **FRAUD-02-06-03** of **section 2.6** in the TDIF 04 Functional Requirements.*

A key method of fraud detection is proactive notification by *Individual*s affected by a *Digital Identity Fraud Incident*. *Applicants* are required to provide a method for *Individuals* to notify them of a *Digital Identity Fraud Incident* which has occurred on their *Identity Facility*. This can be provided using multiple methods, from an online form to a dedicated communications channel for *Individuals* to notify the *Applicant* of potential fraud. The *Applicant* should ensure that they have clear, publicly accessible

instructions for how to access this channel, and that this channel is available for use by the general public, rather than just their *Users*

Applicants should consider leveraging the following resources when providing support services to *Individual*s affected by a *Digital Identity Fraud Incident*:

- The Commonwealth Department of Home Affairs has developed a range of resources to assist *Individual*s to protect their identity and to recover from the effects of identity crime. See: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-protection-recovery
- iDcare is a national support centre for victims of identity crime and offers a free service to assist victims with repairing the damage to their reputation, credit history and identity information. See: https://www.idcare.org//
- The Australian Federal Police provides advice to *Individual*s on strategies to protect themselves from becoming victims of identity crime. See: https://www.afp.gov.au/what-we-do/crime-types/fraud/identity-crime
- The Office of the Australian Information Commissioner (*OAIC*) has information for the steps victims of identity fraud can take to minimise further damage. See: https://www.oaic.gov.au/privacy/data-breaches/identity-fraud/

Privacy Guidance

General privacy guidance

Relates to TDIF requirements ***PRIV-03-01-01*** *to* ***PRIV-03-01-02*** *of* ***section 3.1*** *in the TDIF 04 Functional Requirements.*

Applicants need to protect all information comprising:

- 'Personal information' as defined by the *Privacy Act 1988 (Cth)* or Australian state or territory government jurisdictional legislation.
- Information about an *Individual* who has died.
- Where the *Identity Service Provider* is a state or territory government agency, personal information as defined by a relevant state jurisdiction.
- The data created and retained about the *attributes* disclosed by an *Identity Exchange*.

Sources:
The Office of the Australian Information Commissioner (*OAIC)* website has valuable guidance for privacy that are referenced throughout the TDIF requirements and Guidance documents. See: https://www.oaic.gov.au/privacy/

The *Australian Privacy Principles guidelines* are available on the *OAIC* website. See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/

If an *Applicant* wants to opt-in to the coverage of the *Privacy Act 1988* (Cth), the *Applicant* can complete a formal process by filling out an application form and providing details of its *Privacy Policy* to the *OAIC*. Further information about the opt-in process, and copies of the relevant forms, can be found on the *OAIC's* website. See: https://www.oaic.gov.au/privacy/privacy-registers/privacy-opt-in-register/opting-in-to-the-privacy-act/

Privacy governance

Privacy Roles

*Relates to TDIF requirements **PRIV-03-02-01** to **PRIV-03-02-02b** of **section 3.2.1** in the TDIF 04 Functional Requirements.*

An *Applicant's* designated *Privacy Officer,* who is the primary point of contact for advice on privacy matters, can also be its designated *Privacy Champion*. *Privacy Officers* play a vital role in promoting strong privacy governance and capability in their respective organisations – helping build public confidence that information is being respected and protected.

The Australian Government Agencies Privacy Code has more detail on the roles of a *Privacy Officer* and *Privacy Champion*. See: https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code/

The *OAIC Privacy Officer Toolkit* contains a number of resources to assist *Applicants* in understanding and performing privacy roles and functions. See: https://www.oaic.gov.au/s/privacy-officer-toolkit/

Privacy Policy

*Relates to TDIF requirements **PRIV-03-02-03** to **PRIV-03-02-05** of **section 3.2.2** in the TDIF 04 Functional Requirements.*

Applicants who apply for accreditation under the *TDIF* need to develop a separate *Privacy Policy* to their other business or agency functions, if applicable.

A *Guide to developing an APP Privacy Policy* is available from the *OAIC.* See: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-developing-an-app-privacy-policy/

Privacy Management Plan

*Relates to TDIF requirements **PRIV-03-02-06** and **PRIV-03-02-07** of **section 3.2.3** in the TDIF 04 Functional Requirements.*

A *Privacy Management Plan* is a document that identifies specific measurable privacy goals and targets and sets out how *Applicants* will meet their compliance obligations under the Australian Privacy Principles 1.2.

An Interactive *Privacy Management Plan* tool is available from the *OAIC.* See: https://www.oaic.gov.au/privacy/guidance-and-advice/interactive-privacy-management-plan-for-agencies/

Privacy awareness training

*Relates to TDIF requirements **PRIV-03-02-08** and **PRIV-03-02-09** of **section 3.2.4** in the TDIF 04 Functional Requirements.*

Privacy training will assist *personnel* to understand their responsibilities and avoid practices that would breach privacy obligations. Training should consider new starters, contractors and temporary staff.

An *Applicant's personnel* should understand the *Applicant*'s *Privacy Policy*, any relevant TDIF privacy requirements, and relevant Privacy laws. Additionally, it is recommended that training covers the importance of good information handling practices and should keep up to date with changes in privacy law and technology.

The *OAIC Guide to Securing Personal Information* [Personal Security and Training section] incorporates advice on considerations to include when developing training resources. See: https://www.oaic.gov.au/s/privacy-officer-toolkit/

Privacy Impact Assessment (PIA)

*Relates to TDIF requirements **PRIV-03-03-01** to **PRIV-03-03-01b** of **section 3.3** in the TDIF 04 Functional Requirements.*

A *PIA* needs to be conducted for all *High Risk Projects* related to an *Applicant's Identity System*. As defined in the *TDIF 01 Glossary of Abbreviations and Terms*, a *High Risk project* is:

> A change to the services for which the entity is accredited or the entity's *Identity System* that is or is likely to have a significant impact on:

- the nature or scope of personal information collected, stored or processed by the entity; or
- the manner in which personal information is collected, stored or processed by the entity.

*Applicant*s must consider if any planned updates or new feature implementations to their *Identity System* meet the definition above.

*Applicant*s should also note that *Finance* will request and assess any PIAs conducted on *High Risk Projects* as part of an *Applicant's Annual Assessment*. Further information, including requirements, can be found in *TDIF 07 Maintain Accreditation*. See: Trusted Digital Identity Framework (TDIF) | Digital Identity

A *Guide to undertaking privacy impact assessments* is available from the *OAIC*. See: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/.

A template for a *PIA* is available on the *Digital Identity* website. See: Trusted Digital Identity Framework (TDIF) | Digital Identity

Data Breach Response Management

*Relates to TDIF requirements **PRIV-03-04-01** to **PRIV-03-04-03** of **section 3.4** in the TDIF 04 Functional Requirements.*

An eligible *Data Breach* is a *Data Breach* that is likely to result in serious harm to any of the *Individual*s to whom the information relates. The OAIC guidance sets out that an eligible *Data Breach* arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of *personal information*, or a loss of *personal information*, that an entity holds
2. this is likely to result in serious harm to one or more *Individual*s, and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

Further information on how to assess whether an eligible *Data Breach* has occurred can be found on the OAIC's guidance *Part 4: Notifiable Data Breach (NDB) Scheme*. See: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-

and-response/part-4-notifiable-data-breach-ndb-scheme#identifying-eligible-data-breaches.

A *Data Breach Response Plan* is a tool to help *Applicants* prepare for, respond to and limit the consequences of a *Data Breach*.

The *Data Breach* preparation and response guide available from the *OAIC* includes guidelines on preparing a *Data Breach Response Plan*. See: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-2-preparing-a-data-breach-response-plan

The *Data Breach Response Plan* must also be consistent with an *Applicant's Digital Identity Fraud Control Plan* and the *System Security Plan*. It is recommended that an *Applicant* considers liaising with members of its security teams in the event of a *Data Breach* to ensure it addresses any resulting privacy and security risks together.

Notification of Collection

Relates to TDIF requirement ***PRIV-03-05-01*** and ***PRIV-03-05-02*** *of* ***section 3.5*** *in the TDIF 04 Functional Requirements.*

Guidance on what information is required in a *Notification of Collection* is available from the *OAIC* in chapter 5 of the *Australian Privacy Principles guidelines.* See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information/

Collection and use limitation

Relates to TDIF requirements ***PRIV-03-06-01*** *to* ***PRIV-03-06-06*** *of* ***section 3.6*** *in the TDIF 04 Functional Requirements.*

Under TDIF Req PRIV-03-06-04a, an *Applicant* must not provide *Personal Information* for enforcement related activities conducted by or on behalf of an *Enforcement Body*. For clarity, an *Applicant* can disclose *Personal Information* to an *Enforcement Body* as part of a referral to investigate a *Cyber Security Incident* or

Digital Identity Fraud Incident under PROT-04-02-10 and FRAUD-02-05-01, respectively.

PRIV-03-06-04a is a general prohibition in place to prevent disclosure of *personal information* where an *Enforcement Body* requests that information to support their enforcement related activities, unless one of the exemptions listed in the requirement applies.

Guidance on collection and use limitation of *personal information* is available from the *OAIC* in chapter 3 the *Australian Privacy Principles guidelines*. See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information/

Collection and disclosure of biometrics

*Relates to TDIF requirements **PRIV-03-08-01** to **PRIV-03-08-03** of **section 3.8** in the TDIF 04 Functional Requirements.*

Biometric Information is defined in the *TDIF 01 Glossary of Abbreviations and Terms*. All *Applicants* must be aware that the TDIF prescribes a narrower scope of information handling requirements for *Biometric Information* than those in the *Privacy Act 1988* (Cth). This is to support the TDIF Principles outlined in *TDIF 02 Overview*.

Destruction of Biometric Information

The TDIF mandates that all *Biometric Information* must be destroyed once the purposes that information was collected for are fulfilled.

- **For IdPs**, this is immediately after the *Biometric Binding* is complete.
- **For CSPs**, this is immediately after an *Individual* withdraws their *Express Consent* for the CSP to hold the *Biometric Information* for *authentication* purposes.

For clarity, if the *Applicant* is an IdP and has collected the *Biometric Information* for *Biometric Binding* processes, this information may be disclosed under PRIV-03-08-01a to an *Accredited* CSP who is collecting that information for the purposes of authenticating the *Individual* to their *Digital Identity*. Furthermore, if the *Applicant*'s *Identity System* is accredited as both an IDP and a CSP, information initially collected for the purposes of *Biometric Binding* can be retained for the purposes of authenticating the *Individual* to their *Digital Identity*.

PRIV-03-08-02a provides an exemption to the destruction of *Biometric Information* if that information was collected for the purposes of creating a government issued *identity document* and the *Applicant* is an *identity document issuer* for that document. For example, a *Road Traffic and Transport Authority* may collect and use the *Biometric Information* to create a drivers licence document if it is an *Identity document issuer* and an *Identity Service Provider*.

A record of the destruction of *Biometric Information* must be maintained by the *Applicant*. *Finance* will request evidence of this record, including evidence that the *Applicant* can demonstrate that any *Biometric Information* held by third-party or sub-contracted components of their *Identity System* is also destroyed. The *Applicant* is responsible for the retention and destruction of all *Biometric Information* collected in accordance with the TDIF requirements.

The nature of the evidence for the destruction of this *Biometric Information* data will be system dependent, as not all systems will be able to provide this evidence in the same way. If an *IdP's* system can generate audit logs associated with deletion, this could constitute sufficient evidence. However, many modern cloud computing environments may not be able to do this and *IdPs* will have to determine system specific evidence to provide certainty that *User's Biometric Information* is being destroyed according to the TDIF's requirements.

PRIV-03-08-04 provides an exemption to the disclosure of *Biometric Information* only if that information is disclosed to the *Individual* to whom it relates. This requirement is not an exemption for the destruction of *Biometric Information* required under PRIV-03-08-02.

Guidance on collecting *sensitive information* is available from the *OAIC* in chapter 3 of the *Australian Privacy Principles guidelines*. See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information/#collecting-sensitive-information

Guidance on collection and disclosure of biometrics is available from the *OAIC* throughout the *Australian Privacy Principles guidelines*. See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/

Biometric Binding requirements for IdPs are located in **Section 3.8** of *TDIF 05 Role Requirements*.

Biometric *Authentication* requirements for CSPs are located in **Section 4.3.3** of *TDIF 05 Role Requirements*.

Consent

*Relates to TDIF requirements **PRIV-03-09-01** to **PRIV-03-09-05** of **section 3.9** in the TDIF 04 Functional Requirements.*

An *Applicant* must ensure Express Consent is obtained from an *Individual* prior to disclosing any of the *Individual*'s Attributes to a *Relying Party* or any third party (including an Authoritative Source).

- **Attribute Service Providers:** An *Attribute Service Provider* is required to obtain *Express Consent* prior to the disclosure of any *Attributes* to a *Relying Party*. If the connection to the *Relying Party* is brokered by an *Identity Exchange*, *Express Consent* may be obtained by the *Identity Exchange* on behalf of the *Attribute Service Provider*.

- **Identity Service Providers:** If the *Identity Service Provider* connects directly with a *Relying Party*, it is required to obtain *Express Consent* prior to the disclosure. If the connection to the *Relying Party* is brokered by an *Identity Exchange*, *Express Consent* may be obtained by the *Identity Exchange* on behalf of the *Identity Service Provider*.

- **Identity Exchange:** If the connection to the *Relying Party* is brokered by an *Identity Exchange*, the *Identity Exchange* may delegate the collection of *Express Consent* to the *Identity Service Provider or Attribute Service Provider*.

Enduring Express Consent

The TDIF recognises that *Applicant*s may collect *Express Consent* that endures for various periods. For example, *Applicant*s may collect *Express Consent* from an *Individual* on a one-off basis for each transaction, or they may collect *Express Consent* that is intended to endure for a certain period of time.

Applicants who do not collect enduring *Express Consent* do not need to meet the enduring *Express Consent* requirements (PRIV-03-09-02a, PRIV-03-09-02b, PRIV03-09-02c 02a, and PRIV-03-09-02d).

Additional guidance for *Consent* is available from the *OAIC* in the *Australian Privacy Principles guidelines.* See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/

Cross border and contractor disclosure of Personal information

Relates to TDIF requirements ***PRIV-03-10-01*** *to* ***PRIV-03-10-02a*** *of* ***section 3.10*** *in the TDIF 04 Functional Requirements.*

Applicants who contract out the operation of a part of its business covered by the *TDIF* requirements are required to provide evidence to *Finance* that it has appropriate contractual and practical measures in place to ensure the contractor is complying with the *TDIF* privacy requirements.

Guidance on cross border and contractor disclosure of *personal information* is available from the *OAIC* in chapter 8 of the *Australian Privacy Principles guidelines.* See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information/

Single Identifiers

Relates to TDIF requirement ***PRIV-03-11-01*** *of* ***section 3.11*** *in the TDIF 04 Functional Requirements.*

An *Applicant* must not create and assign a unique identifier in their *Identity System* to a *User* for use or disclosure across an *Identity Federation*. This means that while *Applicants* can create a unique identifier, this identifier must not be shared with more than one receiving party. *Applicant*s must not pass a unique identifier allocated to a *User's Digital Identity* to multiple *Relying Parties* or other *Accredited Providers.*

This requirement does not prevent an *Applicant* from creating unique identifiers to identify *Users* with a single *Relying Party* or single *Accredited Provider*.

*Applicant*s and *Accredited Providers* should note that this requirement prohibits any received unique identifiers for a User from being passed on to any other *Relying Parties*, third parties, or Accredited Providers across an *Identity Federation*.

This policy is intended to ensure that an *Identity Federation* does not create a unique identifier for an *Individual* to enable profiling of that *Individual*'s online activities. It is intended to help ensure *Individual*'s privacy online and mitigate the potential for data profiling and tracking of the *User* across services.

This requirement only applies to unique identifiers created in the *Applicant's Identity System*. Where the *Applicant* is responsible for the creation of an identifier under a regulatory scheme (such as the *Student Identifiers Act 2014*) this will not be prohibited by the *TDIF*. Where these identifiers are government related, the *Applicant* is instead required to comply with APP 9 for their use of government related identifiers.

Guidance on the adoption, use and disclosure of government related identifiers is available from the *OAIC* in chapter 9 of the Australian Privacy Principles guidelines. See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers/

For an example of implemented approaches to ensuring that an identity can be uniquely distinguished, but not correlated across Services, see the *OpenID Connect 1.0* standard and its use of *pairwise identifiers.*

Access and correction

*Relates to TDIF requirements **PRIV-03-12-01** to **PRIV-03-12-07a** of **section 3.12** in the TDIF 04 Functional Requirements.*

Guidance on access and correction of *Personal Information* is available from the *OAIC* in chapter 12 of the *Australian Privacy Principles Guidelines.* See: *https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-12-app-12-access-to-personal-information/*

Quality of personal information

*Relates to TDIF requirements **PRIV-03-13-01** to **PRIV-03-13-03** of **section 3.13** in the TDIF 04 Functional Requirements.*

Applicants must take reasonable steps to ensure the quality of *personal information* at two distinct points in the information handling cycle. The first is at the time the information is collected. The second is at the time the information is used or disclosed.

Guidance on quality of *personal information* is available from the *OAIC* in chapter 10 of the *Australian Privacy Principles guidelines.* See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information/

Handling Privacy Complaints

*Relates to TDIF requirement **PRIV-03-14-01** of **section 3.14** in the TDIF 04 Functional Requirements.*

Guidance, advice and a checklist on how to handle privacy complaints is available from the *OAIC.* See: https://www.oaic.gov.au/privacy/guidance-and-advice/handling-privacy-complaints/

Destruction and de-identification

Relates to TDIF requirement ***PRIV-03-15-01*** *of* ***section 3.15*** *in the TDIF 04 Functional Requirements.*

There are various legislative regimes in Australia that prescribe specific time frames for records retention and destruction. All records destruction and de-identification is to be undertaken in accordance with applicable laws, regulations and policies, including those defined in the *Archives Act 1983* (Cth) and *Privacy Act 1988* (Cth).

If an *Applicant* de-identifies *Personal Information*, *Applicants* or third parties should not be able to re-identify data through public or other sources and *Applicant*s must take reasonable steps to ensure this does not occur.

Chapter 11 of the *Australian Privacy Principles guidelines* contains further information regarding AP11.2. See: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/

Additional guidance on the destruction and de-identification of records is available from the *OAIC* at: https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/

Protective Security Guidance

The TDIF protective security requirements ensure *Applicants* establish a minimum protective security baseline for their *Identity System* and align with security advice, guidance, policies and publications developed by the Australian Government. This includes the *Australian Government Protective Security Policy Framework* (*PSPF*) and the *Australian Government Investigations Standards (AGIS)* developed by the Australian Government *Attorney General's Department,* as well as the *Australian Government Information Security Manual* (*ISM*) developed by the *Australian Cyber Security Centre* (*ACSC*).

While these policies and standards were developed for use by Australian Government entities, they contain useful guidance and information that may aid commercial and other jurisdiction government *Applicants* during their TDIF accreditation. An *Applicant* should consider these standards as guidance for implementing the TDIF Protective Security Requirements, and any reference to them in this document should be taken as such.

Applicants that undergo the *TDIF Accreditation Process* should note the following:

- Refences to 'entities', 'agencies', 'accountable authority' and 'Australian Government' in the *PSPF*, *AGIS* or *ISM* are to be interpreted as references to the *Applicant*.
- The scope of requirements are limited to the *Identity System* being accredited and not to the *Applicant's* wider operating environment.
- At a minimum, the *Applicant* must handle all information as *OFFICIAL information* unless the *Applicant* has determined a higher security classification is required. See the *PSPF* (INFOSEC-08 - Sensitive and classified information) for further information on the sensitive and security classification of information.

For *Applicants* who are required to comply with the below standards, to the extent of any conflict between:

- Any requirement in the *TDIF* protective security requirements and the current edition of the *PSPF*, then the *PSPF* takes precedence.

- Any requirement listed in the *TDIF* protective security requirements and the current edition of the *ISM*, then the *ISM* takes precedence.
- Any requirement in the *TDIF* protective security requirements and the current edition of the *AGIS*, then the *AGIS* takes precedence.

An *Applicant* may be subject to equivalent state or territory requirements for the above standards. In general, the *TDIF* does not override any legislative or regulatory requirements that are applicable to the *Applicant.*

The *PSPF* articulates government protective security policy. It also provides guidance to support the effective implementation of the policy across the areas of security governance, personnel security, physical security and information security. The *PSPF* is applied through a security risk management approach, with a focus on fostering a positive culture of security within the entity and across the government.

Sources:
A copy of the *PSPF* is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/.
A copy of the *AGIS* is available from the Attorney-General's Department. See: https://www.ag.gov.au/integrity/publications/australian-government-investigations-standards-2011
The latest version of the ISM is available from the Australian Signals Directorate. See: https://www.cyber.gov.au/ism

Security governance

*Relates to the TDIF requirements in **section 4.1** of the TDIF 04 Functional Requirements.*

Security governance ensures each *Applicant* manages security risks and supports a positive security culture in an appropriately mature manner.

General

*Relates to TDIF requirements **PROT-04-01-01** to **PROT-04-01-03** of **section 4.1.2** in the TDIF 04 Functional Requirements.*

For Australian Government entities, the requirements in this section are intended to be similar to the obligations placed by the *PSPF* on their accountable authority.

The *PSPF GOVSEC-01 (Role of the Accountable Authority)* includes guidance for the role and responsibilities of the accountable authority. This guidance is also relevant to the role and responsibilities these requirements place on the *Applicant.*

It also describes ways to establish consistent, efficient and effective protective security measures across the *Applicant's* operations. These measures form a basis for protecting *Personnel*, information (including *ICT*) and assets from security threats and supports the continuous delivery of the *Applicant's* business.

The core requirements of *GOVSEC-01* stipulate that the accountable authority of each entity must:

a) determine their entity's tolerance for security risks
b) manage the security risks of their entity
c) consider the implications their risk management decisions have for other entities and share information on risks where appropriate.

The accountable authority of a lead security entity must:

a) provide other entities with advice, guidance and services related to government security
b) ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security
c) establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities.

The *PSPF* (*GOVSEC-01 - Role of the Accountable Authority*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-1-role-of-accountable-authority.pdf

The assessment of the *Cyber Security Risk* under PROT-04-01-01 should use the best available information, supplemented by the views of stakeholders and further enquiry as necessary. **Appendix A: Potential Sources of Risk** of this document provides a list of some potential sources of risk that *Applicants* should consider when undergoing this assessment of *Cyber Security Risk*. See the ***Digital Identity* Risk**

Management section of this document for further guidance as to conducting this assessment.

Management structures and responsibilities

*Relates to TDIF requirements **PROT-04-01-04** to **PROT-04-01-10** of **section 4.1.2** in the TDIF 04 Functional Requirements.*

The *PSPF GOVSEC-02 (Management structures and responsibilities)* includes guidance for the preferred management structures and responsibilities that determine how security decisions are made in accordance with security practices. This provides a governance base for *Applicants* to protect their people, information, *ICT* and assets and will assist in enabling the *Applicant* to achieve security outcomes.

The core requirements of *GOVSEC-02* stipulate that the *Accountable Authority* must:

a) appoint a *Chief Security Officer (CSO)* at the Senior Executive Service level to be responsible for security in the entity
b) empower the *CSO* to make decisions about:
    i. appointing security advisors within the entity
    ii. the entity's protective security planning
    iii. the entity's protective security practices and procedures
    iv. investigating, responding to, and reporting on security incidents.
c) ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture and are provided sufficient information and training to support this.

The *PSPF* (*GOVSEC-02 – Management structures and responsibilities*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/system/files/2021-08/PSPF-policy-2-Management-structures-and-responsibilities.pdf

System Security Plan

*Relates to TDIF requirements **PROT-04-01-11** to **PROT-04-01-14** of **section 4.1.3** in the TDIF 04 Functional Requirements.*

The *PSPF GOVSEC-03 (Security planning and risk management)* includes guidance for *Applicants* on how to establish effective security planning and embed security into risk management practices.

Security planning can be used to identify and manage risks and assist decision-making by:

- Applying appropriate controls effectively and consistently (as part of the *Applicant's* existing risk management arrangements)
- Adapting to change while safeguarding the delivery of business and services
- Improving resilience to threats, vulnerabilities and challenges
- Driving protective security performance improvements.

The core requirements of *GOVSEC-03* stipulate that each entity must have in place a security plan approved by the *A*ccountable *A*uthority to manage the entity's security risks. The security plan details the:

a) security goals and strategic objectives of the *entity*, including how security risk management intersects with and supports broader business objectives and priorities
b) threats, risks and vulnerabilities that impact the operation of the *entity's Identity Systems*
c) *entity's* tolerance to security risks
d) maturity of the *entity's* capability to manage security risks
e) *entity's* strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.

The *PSPF* (*GOVSEC-03 - Security planning and risk management*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-3-security-planning-and-risk-management.pdf

Security maturity monitoring

*Relates to TDIF requirements **PROT-04-01-19** and **PROT-04-01-19a** of **section 4.1.4** in the TDIF 04 Functional Requirements.*

The *PSPF GOVSEC-04 (Security maturity monitoring)* describes security maturity monitoring and includes guidance for *Applicants* on how to monitor and assess the maturity of its security capability and risk culture. This includes the *Applicant's* capability to actively respond to emerging threats and changes in its security environment, while maintaining the protection of its people, information (including *ICT*) and assets.

The core requirements of *GOVSEC-04* stipulate that each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan.

The *PSPF* (*GOVSEC-04 – Security maturity monitoring*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-4-security-maturity-monitoring.pdf

Information Security

*Relates to TDIF requirements **PROT-04-02-01** to **PROT-04-02-29** of **section 4.2** in the TDIF 04 Functional Requirements.*

The purpose of the *ISM* is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats. It sets out cyber security guidelines that will assist *Applicants* to meet the requirements of *TDIF* accreditation.

A copy of the *ISM* is available from the Australian Signals Directorate. See: https://www.cyber.gov.au/ism

Sensitive and classified information

*Relates to TDIF requirements **PROT-04-02-01** and **PROT-04-02-02** of **section 4.2.1** in the TDIF 04 Functional Requirements.*

The *PSPF INFOSEC-8 (Sensitive and classified information)* includes guidance for *Applicants* on how to assess the sensitivity of their information and adopt marking, handling, storage and disposal arrangements that guard against information compromise. Information is a valuable resource. Protecting the confidentiality, integrity and availability of information is critical to business operations.

- Confidentiality of information refers to the limiting of access to information to *Individuals* and authorised *Personnel* for approved purposes (*Need-to-know*).
- Integrity of information refers to the assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid.
- Availability of information refers to allowing *Individuals* and authorised *Personnel* to access information for authorised purposes at the time they need to do so.

The core requirements of *INFOSEC-08* stipulate that each entity must:

a) identify information holdings
b) assess the sensitivity and security classification of information holdings
c) implement operational controls for these information holdings proportional to their value, importance and sensitivity.

The *PSPF* (INFOSEC-08 – Sensitive and classified information) is available from the Attorney-General's Department. See:
https://www.protectivesecurity.gov.au/system/files/2022-03/pspf-policy-08-sensitive-and-classified-information.pdf

Access to information

*Relates to TDIF requirements **PROT-04-02-03** and **PROT-04-02-04a** of **section 4.2.2** in the TDIF 04 Functional Requirements.*

The *PSPF INFOSEC-09 (Access to Information)* includes guidance on security protections that support the *Applicant's* provision of timely, reliable and appropriate access to information. Providing access to information helps develop new products and services, can enhance consumer and business outcomes and assists with decision making and policy development.

The core requirements of *INFOSEC-09* stipulate that *Applicants* must enable appropriate access to official information. This includes:

a) sharing information within the entity, as well as with other relevant stakeholders
b) ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information
c) controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.

The *PSPF* (*INFOSEC-09 - Access to information*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/system/files/2021-11/PSPF%20Policy%2009%20-%20Access%20to%20information.pd f

Safeguarding information from cyber threats

*Relates to TDIF requirements **PROT-04-02-05** to **PROT-04-02-06** of **section 4.2.3** in the TDIF 04 Functional Requirements.*

The *PSPF INFOSEC-10* (*Safeguarding information from cyber threats*) describes how to safeguard information from cyber threats and details how *Applicants* can mitigate common and emerging cyber threats, which may include:

- External *malicious actors* who steal data
- Ransomware that denies access to data and external *malicious actors* who destroy data and prevent systems from functioning
- Malicious insiders who steal data
- Malicious insiders who destroy data and prevent systems from functioning.

The core requirements in *INFOSEC-10* stipulate:

Each entity must mitigate common and emerging cyber threats by:

a) implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents:
    i. application control
    ii. patching applications
    iii. restricting administrative privileges
    iv. patching operating systems.
b) considering which of the remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents you need to implement to protect your entity.

The *PSPF* (*INFOSEC-10 - Safeguarding information from cyber threats*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/sites/default/files/2019-11/pspf-infosec-10-safeguarding-information-cyber-threats.pdf

The most common cyber threat facing *Applicants* is external *Malicious Actors* who attempt to steal data. Often these *Malicious Actors* want to access systems and information through email and web pages. It is critical that *Applicants* safeguard the information held on systems that can receive emails or browse internet content.

The *ACSC* provides expert security guidance to help agencies and organisations mitigate cyber threats. While no single mitigation strategy is guaranteed to prevent a security incident, the *ACSC* estimates many cyber threats could be mitigated by whitelisting applications, patching applications and operating systems and restricting administrative privileges. These four strategies form part of the *Essential Eight* mitigation strategies.

While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline. The Australian Cyber Security Centre has identified these mitigation strategies, which are known as the *Essential Eight.* This baseline makes it much harder for adversaries to compromise systems. Furthermore, implementing the *Essential Eight* proactively can be more cost-effective in terms of time, money and effort than having to respond to a large-scale *cyber security incident*. The *TDIF* recommends that the *Applicant* considers implementing these strategies as part of the development of their *Identity System*.

A summary of the *Essential Eight* mitigation strategies is:

- **Application control** – to prevent execution of unapproved/malicious programs. By doing this, all non-approved applications (including malicious code) are prevented from executing.
- **Patch applications** – including Flash, web browsers, Microsoft Office, Java and PDF viewers. Security vulnerabilities in applications can be used to execute malicious code on systems.
- **Configure Microsoft Office macro settings** – to block macros from the internet and only allowing vetted macros from 'trusted locations'. Microsoft Office macros can be used to deliver and execute malicious code on systems.
- **User application hardening** – for example configuring web browsers to block Flash, ads and Java on the internet and disabling unneeded features in Microsoft Office. Flash, ads and Java are popular ways to deliver and execute malicious code on systems.
- **Restrict administrative privileges** – to operating systems and applications based on user duties. Admin accounts are the 'keys to the kingdom', adversaries use these accounts to gain full access to information and systems.
- **Patch operating systems** – security vulnerabilities in operating systems can be used to further the compromise of systems.
- **Multi-factor authentication** – stronger user authentication makes it harder for adversaries to access sensitive information and systems
- **Daily backups** – to ensure information can be accessed following a cyber security incident (e.g. a ransomware incident).

The *ACSC* website has further information on the *Essential Eight*. See: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained

The Australian Cyber Security Centre website has further information on strategies to mitigate cyber security incidents. See: https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

Incident management, investigations and reporting

*Relates to TDIF requirements **PROT-04-02-07** to **PROT-04-02-14a** of **section 4.2.4** in the TDIF 04 Functional Requirements.*

The incident management requirements in the TDIF are focused on ensuring that an *Applicant* has sufficient mechanisms to detect and respond to *Cyber Security Incidents* This includes making provision for referring investigation of incidents to *Enforcement bodies*. If an incident is referred to and accepted by an *Enforcement Body* or the Australian Cyber Security Centre, the *Applicant* should provide support and any relevant materials necessary for that body to conduct the investigation.

For further guidance on managing investigations into *Cyber Security Incidents*, see the *Australian Government Investigation Standards*. See: https://www.ag.gov.au/integrity/publications/australian-government-investigations-standards-2011

Support for victims of security incidents

*Relates to TDIF requirements **PROT-04-02-15** to **PROT-04-02-18** of **section 4.2.6** in the TDIF 04 Functional Requirements.*

A key method for mitigating cyber security threats is proactive notification by *Individual*s who suspect or become aware of a *Cyber Security Incident*. *Applicants* are required to provide a method for *Individual*s to notify them of a *Cyber Security Incident* which has occurred on their *Identity Facility*. This can be provided using multiple methods, from an online form, to providing a dedicated communications channel for *Individual*s to notify the *Applicant* of potential incidents. The *Applicant* should ensure that they have clear, publicly accessible instructions for how to access this channel, and that this channel is available for use by the general public, rather than just their *Users*.

Applicants should consider leveraging the following resources when providing support services to *Individual*s affected by a *Cyber Security Incident*:

- The Commonwealth Department of Home Affairs has developed a range of resources to assist *Individual*s to protect their identity and to recover from the effects of identity crime. See: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-protection-recovery
- iDcare is a national support centre for victims of identity crime and offers a free service to assist victims with repairing the damage to their reputation, credit history and identity information.. See: https://www.idcare.org//
- The Australian Federal Police provides advice to *Individual*s on strategies to protect themselves from becoming victims of identity crime. See: https://www.afp.gov.au/what-we-do/crime-types/fraud/identity-crime
- The Office of the Australian Information Commissioner (*OAIC*) has information for the steps victims of identity fraud can take to minimise further damage. See: https://www.oaic.gov.au/privacy/data-breaches/identity-fraud/

Where the *Cyber Security Incident* may involve personal information please refer to the guidance in this document on Data Breach response management.

Robust ICT Systems

*Relates to TDIF requirements **PROT-04-02-19** to **PROT-04-02-23a** of **section 4.2.6** in the TDIF 04 Functional Requirements.*

The *PSPF INFOSEC-11 (Robust ICT systems)* provides guidance on how *Applicants* can safeguard *ICT* systems to support the secure and continuous delivery of their identity service. Secure *ICT* systems protect the integrity (and facilitate the availability) of the information that the *Applicant* processes, stores and communicates.

The core requirement of *INFOSEC-11* stipulates that each entity must have in place security measures during all stages of *ICT* systems development. This includes certifying and accrediting *ICT* systems in accordance with the *Information Security Manual* when implemented into the operational environment.

The *PSPF (INFOSEC-11 – Robust ICT systems*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-11-robust-ict-systems.pdf

Disaster recovery and business continuity management

*Relates to TDIF requirements **PROT-04-02-24** and **PROT-04-02-25** of **section 4.2.7** in the TDIF Functional requirements document.*

The development of a *Disaster Recovery and Business Continuity Management Plan* (*DRBCP*) helps minimise the disruption to the availability of information and systems after a security incident or disaster by documenting the response procedures.

Developing a *DRBCP* will reduce the time between a disaster occurring and critical functions of systems being restored. A *DRBCP* can help ensure that critical functions of systems continue to operate when the system is in a degraded state.

The Australian Government's business.gov.au website has additional information and resources for creating a *DMBCR.* See: https://business.gov.au/Risk-management/Emergency-management/How-to-prepare-an-emergency-management-plan

The *DMBCR* template developed by the Queensland Government outlines things to consider in the Business Continuity Planning Process and includes guidance throughout. See: https://www.publications.qld.gov.au/dataset/business-continuity-planning-template .

Cryptography

*Relates to TDIF requirements **PROT-04-02-26** to **PROT-04-02-27** of **section 4.2.8** in the TDIF 04 Functional Requirements.*

There is no guarantee of a cryptographic algorithm's resistance against currently unknown attacks. However, the algorithms listed in the cryptographic section of the *ISM* have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any

feasible attacks. There have been some cases where theoretically impressive security vulnerabilities have been found; however, these results are not of practical application.

The Australian Signals Directorate (*ASD*) *Approved Cryptographic Algorithms* (*AACAs*) fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms.

The current approved asymmetric/public key algorithms are:

- Diffie-Hellman (DH) for agreeing on encryption session keys
- Digital Signature Algorithm (DSA) for digital signatures
- Elliptic Curve Diffie-Hellman (ECDH) for key exchange
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures
- Rivest-Shamir-Adleman (RSA) for digital signatures and passing encryption session keys or similar keys

The approved hashing algorithm is Secure Hashing Algorithm 2 (SHA-2) (i.e. SHA-224, SHA-256, SHA-384 and SHA-512).

The approved symmetric encryption algorithms are Advanced Encryption Standard (AES) using key lengths of 128, 192 and 256 bits, and Triple Data Encryption Standard (3DES) using three distinct keys.

In general, ASD only approves the use of cryptographic equipment and software that has passed a formal evaluation. However, ASD approves the use of some cryptographic protocols even though their implementations in specific cryptographic equipment or software has not been formally evaluated by ASD. This approval is limited to cases where they are used in accordance with these guidelines.

As of the time of publication, the *ASD approved cryptographic protocols* (*AACPs*) currently listed in the ISM are:

- Transport Layer Security (TLS)
- Secure Shell (SSH)
- Secure/Multipurpose Internet Mail Extension (S/MIME)
- OpenPGP Message Format
- Internet Protocol Security (IPsec)

- Wi-Fi Protected Access 2 (WPA2).

The *ACSC* website has further information regarding the latest *AACAs.* See: https://www.cyber.gov.au/acsc/view-all-content/guidance/asd-approved-cryptographic-algorithms

Cryptographic Key Management Plan

Key management is described as the use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.

A *Cryptographic Key Management Plan* (*CKMP*) identifies the implementation, standards, procedures and methods for key management in *PKI* service providers and provides a good starting point for the protection of cryptographic systems, keys and digital certificates.

An *Applicant*'s *CKMP* should include, at a minimum:

a. Objectives of the cryptographic system and CKMP, including Service Provider aims
b. Accounting:
    i. How accounting will be undertaken for the cryptographic system
    ii. What records will be maintained
    iii. How records will be audited
c. Cyber Security Incidents:
    i. A description of the conditions under which compromise of keys should be declared
    ii. References to procedures to be followed when reporting and dealing with compromised keys
d. Key Management:
    i. How keys are generated
    ii. How keys are delivered to intended users
    iii. How keys are received, installed and activated
    iv. Key distribution, including local, remote and central
    v. How keys are transferred, stored, backed up and archived

vi. How keys are recovered as part of disaster recovery of business continuity management
vii. How keys are revoked, suspended, deactivated and destroyed
viii. How keys are changed or updated
ix. Logging and auditing of key management related activities

e. Maintenance:
   i. Maintaining the cryptographic system software and hardware
   ii. Destroying cryptographic equipment and media
f. References:
   i. Vendor documentation
   ii. Relevant policies
g. Sensitivity or classification of the cryptographic system hardware, software and documentation
h. System description:
   i. Sensitivity or classification of information protected
   ii. The use of keys
   iii. The environment
   iv. Administrative responsibilities
   v. Key algorithms
   vi. Key lengths
   vii. Key lifetime
i. Topology Diagrams and descriptions of the cryptographic system topology including

A template for a *CKMP* is available on the *Digital Identity* website. See: https://www.digitalidentity.gov.au/tdif

Personnel security

Personnel security enables each *Applicant* to ensure its *Personnel* are suitable to access information (including *ICT*) and assets and meet an appropriate standard of integrity and honesty.

Eligibility and suitability of personnel

*Relates to TDIF requirements **PROT-04-03-01** and **PROT-04-03-02** of **section 4.3.1** in the TDIF 04 Functional Requirements.*

The *PSPF PERSEC-12 (Eligibility and suitability of personnel)* provides guidance on managing *Personnel* eligibility and suitability risk and details the pre-employment screening and standardised practices to be undertaken when employing *Personnel*. These processes provide a high-quality and consistent approach to managing *Personnel* eligibility and suitability.

The core requirements of *PERSEC-12* stipulate that each entity must ensure the eligibility and suitability of its personnel who have access to the *Applicant's* resources (people, information and assets).

The *PSPF* (*PERSEC-12 – Eligibility and suitability of personnel*) is available from the Attorney-General's Department. See:
https://www.protectivesecurity.gov.au/system/files/2021-11/PSPF%20policy%2012%20-%20Eligibility-and-suitability-of-personnel.pdf

Ongoing assessment of personnel

*Relates to TDIF requirements **PROT-04-03-03** of **section 4.3.2** in the TDIF 04 Functional Requirements.*

The *PSPF PERSEC-13 (Ongoing assessment of personnel)* provides guidance on how *Applicants* can maintain confidence in their *Personnel's* ongoing suitability to access information (including *ICT*) and assets and manage the risk of malicious or unwitting insiders. It is critical that *Applicants* are aware of changes in their employees' and contractors' circumstances and workforce behaviours. This awareness is facilitated by effective information sharing and a positive security culture, recognising that security is everyone's responsibility.

The core requirement of *PERSEC - 13* stipulates that each entity must assess and manage the ongoing suitability of its *Personnel* and share relevant information of security concern, where appropriate.

The *PSPF* (*PERSEC-13 – Ongoing assessment of personnel*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/system/files/2021-11/PSPF%20policy%2013%20-%20Ongoing-assessment-of-personnel.pdf

Separating personnel

*Relates to TDIF requirements **PROT-04-03-04** to **PROT-04-03-05a** of **section 4.3.3** in the TDIF 04 Functional Requirements.*

The *PSPF PERSEC-14 (Separating personnel)* provides guidance on processes to protect the *Applicant's Personnel*, information and assets when *Personnel* permanently or temporarily leave their employment.

Separating *Personnel* includes:

- *Personnel* voluntarily leaving an *Applicant's* employment
- Those whose employment has been terminated for misconduct or other adverse reasons
- *Personnel* transferring temporarily or permanently to another agency or organisation
- Those taking extended leave.

The core requirements of *PERSEC-14* stipulate that each entity must ensure that separating *Personnel*:

a) have their access to the *Applicant's* resources withdrawn, and
b) are informed of any ongoing security obligations.

The *PSPF* (*PERSEC-14 – Separating personnel*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/system/files/2021-08/pspf-policy-14-separating-personnel.pdf

Physical Security

Physical security for *Applicant* resources.

*Relates to TDIF requirements **PROT-04-04-01** to **PROT-04-04-04** of **section 4.4.1** in the TDIF 04 Functional Requirements.*

The *PSPF PHYSEC-15 (Physical security for entity resources)* provides guidance on the physical protections required to safeguard *Personnel*, information and assets (including *ICT* equipment) to minimise or remove security risk.

The *PSPF* (*PHYSEC-15 – Physical security for entity resources*) is available from the Attorney-General's Department. See: https://www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-15-physical-security-for-entity-resources_0.pdf

User Experience Guidance

The objective of the user experience requirements in the *TDIF* is to enable simple and easy-to-use digital experiences that are accessible and voluntary for *Users.*

The user experience of an *Applicant*'s service needs be shaped by accessible content and functionality that clearly communicates and facilitates purpose, intent and relevance.

This is especially true in a transactional context where *Users* need to know and understand at all times:

- where they are in a specific process (and what they should expect from that process)
- where they have come from
- what options, actions or steps they have in front of them (if any)
- the (implicit) consequences of taking those actions or next steps
- an unambiguous signal, feedback and/or response once that action is taken.

User experience can be considered as a sub-set of service design, which is a human-centred design approach that places equal value on the customer experience and the business process -- aiming to create quality customer experiences and seamless service delivery.

The *DTA Digital Service Standard* incorporates 13 criteria that will help guide *Applicants* to design and deliver services that meet the *User* experience requirements of the *TDIF*.

The criteria include the following:

1. **Understand user needs**. Research to develop a deep knowledge of the *Users* and their context for using the service.
2. **Have a multidisciplinary team**. Establish a sustainable multidisciplinary team to design, build, operate and iterate the service, led by an experienced product manager with decision-making responsibility.
3. **Agile and user-centred process**. Design and build the product using the service design and delivery process, taking an agile and user-centred approach.

4. **Understand tools and systems**. Understand the tools and systems required to build, host, operate and measure the service and how to adopt, adapt or procure them.
5. **Make it secure**. Identify the data and information the service will use or create. Put appropriate legal, privacy and security measures in place.
6. **Consistent and responsive design.** Build the service with responsive design methods using common design patterns and the *Style Guide*.
7. **Use open standards and common platforms**. Build using open standards and common platforms where appropriate.
8. **Make source code open**. Make all source code open by default.
9. **Make it accessible**. Ensure the service is accessible to all users regardless of their ability and environment.
10. **Test the service**. Test the service from end to end, in an environment that replicates the live version.
11. **Measure performance**. Measure performance against KPIs set out in the guides. Report on public dashboard.
12. **Do not forget the non-digital experience**. Ensure that people who use the digital service can also use the other available channels if needed, without repetition or confusion.
13. **Encourage everyone to use the digital service**. Encourage users to choose the digital service and consolidate or phase out existing alternative channels where appropriate.

Further information about each criterion of the *DTA Digital Service Standard* is available on the *DTA* website. See: https://www.dta.gov.au/help-and-advice/digital-service-standard/digital-service-standard-criteria

ISO 9241-210: 2019 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems defines usability as “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.”

A product’s usability is defined by its *Users* and their needs. The *Style Manual* recommends designing content based on the ways *Users* are expected to find and consume that content. The *Style Manual* also recommends that any written content

be at an Australian year 7 level. See: https://www.stylemanual.gov.au/accessible-and-inclusive-content/literacy-and-access

Accessibility and inclusion are also closely related to *User* experience and many *accessibility* requirements improve usability, which in turn encourages inclusion and engagement. The *W3C* website has further information and guidance about accessibility and usability. See: https://www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/

Usability guidance

*Relates to TDIF requirements **UX-05-01-01** to **UX-05-01-07** of **section 5.1** in the TDIF 04 Functional Requirements.*

Other available channels

An *Applicant* must demonstrate to *Finance* other available channels it provides to *Users* to assist them in accessing and using its *Identity System*. For example, in the case of an IdP, this may be a helpdesk for Users struggling to use the IdP's service to prove their identity.

An *Applicant* must also demonstrate how its service can provide support to *Individual*s who either can't use a digital service independently or have low digital skills.

Identity verification journey and authentication journey

*Relates to TDIF requirements **UX-05-02-01** to **UX-05-03-01** of **section 5.2 & 5.3** in the TDIF 04 Functional Requirements.*

To meet the *TDIF* requirements for the identity verification journey, *Applicants* should provide upfront information that assists *Users* to follow the process to use their service as simply and safely as possible, including:

- Technical requirements such as internet access and a webcam
- Identity document requirements

- Useful feedback throughout the process, including clear and concise consequences for a User that does not provide the required information during the process.

Usability test plans

*Relates to TDIF requirements **UX-05-04-01** to **UX-05-04-01c** of **section 5.4** in the TDIF 04 Functional Requirements.*

The *DTA Digital Service Standard* has guidance and tools on processes to undertake usability testing. See: https://www.dta.gov.au/help-and-advice/build-and-improve-services

Usability testing

*Relates to TDIF requirements **UX-05-05-01** to **UX-05-05-04a** of **section 5.5** in the TDIF 04 Functional Requirements.*

Limited Exception

UX-05-05-01 provides a limited exception to the requirements in **Sections 5.4.2** and **5.4.3** of *TDIF 04 Functional Requirements* to *Applicant*s whose *Identity System* has no interaction, or limited interaction with *Users* when providing their service.

An example of no interaction with a *User* may be where an *Exchange's* functions sit wholly in the back-end facilitation of a link between a *Relying Party* and *Identity Service Provider*. This type of *Exchange* would have no application or interaction screens for a *User*.

An example of limited interaction with a *User* may be where an *Exchange's* service only has one or two *User* Journey screens that facilitate a link between a *Relying Party* and an *Identity Service Provider*.

In the case of limited interaction, an *Applicant* must determine and justify through a *Risk Assessment* that failing to conduct usability testing will not adversely affect the usability of its *Identity System*. Additionally, the *Applicant* must also take reasonable steps to ensure that *Users* have available channels to be able to submit feedback

about the usability of the *Applicant*'s *Identity System*. This could include an online form, or phone number a *User* can contact to provide feedback. The *Applicant* must demonstrate that it has processes and procedures in place to ensure that any actionable and reasonable feedback can be incorporated into the design of its *Identity System*.

Conducting Usability Testing

Usability testing is a way to see how easy to use something is by testing it with real *Users*. *Users* are asked to complete tasks, typically while being observed by a researcher, to see where they encounter problems and experience confusion. If people encounter similar problems, the usability journey will be iterated to overcome the issues.

An *Applicant* must use experienced *User Researchers* to conduct usability testing of its *Identity System* and it must be done in accordance with the Usability test plan requirements.

Note: A *User Researcher* does not need to be independent of an *Applicant's* organisation to be able to conduct the Usability Testing.

The *DTA Digital Service Standard* has tools and processes to undertake usability testing at. See: https://www.dta.gov.au/help-and-advice/build-and-improve-services

User needs, research and content guides, as well as *accessibility* and inclusivity guides, are available in the *Style Manual*. See: https://www.stylemanual.gov.au/user-needs

Further information about the Annual Usability Testing requirements is available in *TDIF 07 Maintain Accreditation*. *Applicant*s must be aware of ongoing obligations and requirements for usability testing that will be assessed during their *Annual Assessment.*

Accessibility guidance

*Relates to TDIF requirement **UX-05-06-01** of **section 5.6** in the TDIF 04 Functional Requirements.*

It is important to ensure information and services are provided in a non-discriminatory, accessible manner in order for *Applicants* to comply with their requirements and obligations under the *Disability Discrimination Act 1992* (Cth). Accessibility is a subset of usability and while usability implies accessibility; the contrary is not necessarily true.

The *World Wide Web Consortium (W3C)* defines accessibility as a way to address "discriminatory aspects related to equivalent user experience for people with disabilities. Web accessibility means that people with disabilities can equally perceive, understand, navigate, and interact with websites and tools. It also means that they can contribute equally without barriers." Web accessibility includes addressing usability for all types of disabilities that impact access to the web such as visual, auditory, physical, speech, cognitive and neurological disabilities. Adherence to web accessibility principles also benefits elderly *Users*.

The *Web Content Accessibility Guidelines* (*WCAG*) 2.1 covers a wide range of recommendations for making web content more accessible. It also contains guidance for mobile based content and identity services. See: https://www.w3.org/TR/WCAG21/

The Australian Government *Style Manual* contains up-to-date content guides to help design simple, clear and consistent content. It also includes design guidance for accessibility and inclusivity. See: https://guides.service.gov.au/content-guide/

Technical Testing Guidance

*Relates to TDIF requirements **TEST-06-01-01** to **TEST-06-01-07** of **section 6** in the TDIF 04 Functional Requirements.*

Section 6 of the *TDIF 04 Functional Requirements* sets out the evidence that an *Applicant* is required to provide in order to demonstrate that they have tested the capability of their system to satisfy certain specified requirements.

In addition to the requirements outlined in **section 6**, *Applicants* who are onboarding to the *Australian Government's Digital Identity System* will also need to conduct *Technical Testing* to demonstrate their compliance with the *TDIF 06 Federation Onboarding Requirements* in accordance with FED-02-01-05 and FED-02-02-01.

The TDIF does not prescribe a particular testing regime and is aimed at ensuring that *Applicants* can utilise existing testing processes to satisfy the *TDIF Requirements.* The focus of these requirements is on ensuring that *Finance* is provided with sufficient evidence to assess whether the *Applicant's Identity System* has implemented the stated requirements.

The *Applicant* is required to provide *Finance* with visibility of the processes used by the *Applicant* to test that their system is capable of meeting the specified *TDIF requirements*. The *Applicant's* overarching approach to *Technical Testing* does not need to be agreed upon with *Finance*; however, *Finance* may raise any concerns they have with the approach to testing their system as part of the *Accreditation Process*.

Applicants are also required to develop a *Requirements Traceability Matrix* which documents the links between the requirements they are required to test and the test cases which have been developed to verify and validate those requirements. Test cases detailing the specific steps and expected results are written to validate that all requirements have been met and that the system functions as specified in the design documentation. Test cases may provide evidence of conformance to more than one requirement.

Exit criteria refers to the criteria which the *Applicant* used to determine that the system has satisfied their requirements. This may include criteria regarding the pass rates and the execution coverage. An example of exit criteria for an *Applicant* undergoing risk-based testing would be:

a) The pass rate for all test cases exceeds 95%
b) All Test Incidents and defects uncovered during testing have been documented
c) There are no open defects

During test execution, the *Applicant* should record and retain the actual results, in real time, as evidence of execution. Part of this record needs to include the status for each test case and must be included in the *Technical Test Report*.

Functional Assessments Guidance

*Relates to TDIF requirements **ASSESS-07-01-01** to **ASSESS-07-07-02** of **section 7** in the TDIF 04 Functional Requirements.*

All *Applicant*s must undergo a series a series of *Functional Assessment*s conducted by a relevant *Assessor*.

A *Functional Assessment* refers to an assessment of the *Applicant*'s *Identity System* conducted by an experienced and independent ***Assessor***. The *Assessor* should conduct the *Functional Assessment* and prepare a report, including all the following information:

- The *Applicant's* written instructions as per ASSESS-07-01-02
- Document reviews, interviews with key personnel, and a run through the *Applicant's Identity System*, as per ASSESS-07-03-02
- Outcomes of the *Functional Assessment* as per ASSESS-07-03-04

It is the *Applicant's* responsibility to ensure that the *Assessor* has all information required to prepare their report on the outcomes of the *Functional Assessment*.

A *Functional Assessment Report* refers to a report prepared by the ***Applicant* on the *Functional Assessment***. The *Functional Assessment Report* is a summary of and response to the *Functional Assessment* results and any risks, non-compliances and recommendations that the *Assessor* has identified. A *Functional Assessment Report* must be prepared for each separate *Functional Assessment* and include:

- All information as per ASSESS-07-04-01
- An assessment of each risk, non-compliance and recommendation identified by the *Assessor* as per ASSESS-07-04-02 (if any). Each of these assessments must be assigned a risk rating as set out in **Appendix A: Risk Ratings** of *TDIF 04 Functional Requirements*.
- If an *Assessor* has identified recommendations, risks or non-compliances, then the *Applicant*'s *Accountable Executive* must respond as per ASSESS-07-04-03. A response to an accepted risk, recommendation or non-compliance must include:

    - Actions the *Applicant* will take for implementation of a fix or mitigations to address the recommendation, risk, or non-compliance.
    - A date for when the implementation is to be completed.
- *Applicant*s must consider requirements ASSESS-07-04-03a and ASSESS-07-04-03b when preparing the *Functional Assessment Report*.

Templates for each *Functional Assessment Report* are available on the *Digital Identity* website. See: https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework

Assessor skills, experience and independence

*Relates to TDIF requirements **ASSESS-07-02-01** and **ASSESS-07-02-02** of **section 7.2** in the TDIF 04 Functional Requirements.*

An *Applicant* is required to engage appropriate Assessors to conduct *Functional Assessments*. *Finance* does not maintain a list of Assessors for *Applicants* to use. As part of good corporate governance, the *Applicant* must research, identify and engage appropriate *Assessors* with the relevant skills, experience, independence and qualifications to undertake the required *Functional Assessment.*

Applicants are encouraged to contact several *Assessors* to get a sense of the cost, duration and complexity of the work to be undertaken to complete a *Functional Assessment*.

The following text is provided as guidance to engaging *Assessor*s for the following *Functional Assessments*:

- ***Security Assessments*** can be undertaken by a security advisor, *IRAP Assessor* or other security professional that has relevant, reasonable and adequate experience, training and qualifications to undertake the assessment.
    - CREST can provide further information regarding information and cyber security *Assessor* skills, training and qualifications. See: https://www.crest-approved.org/knowledge-sharing/implementation-procurement-guides/index.html
    - The *Australian Signals Directorate* publishes a list of endorsed qualified ICT security professionals that are registered under the Information

Security Registered *Assessor*s Program (*IRAP*) to provide information security services. See: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-*Assessor*s

- ***Penetration tests*** must be undertaken by organisations or *Individual*s with relevant experience in *penetration testing*.
    - CREST can provide further information regarding information and cyber security *Assessor* skills, training and qualifications. See: https://www.crest-approved.org/knowledge-sharing/implementation-procurement-guides/index.html
- ***Privacy Impact Assessments*** (PIAs) can be undertaken by an independent *Assessor* within the *Applicant's* organisation or an external *Assessor* in accordance with the Office of the Australian Information Commissioner (OAIC) guidelines. https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/.
- ***Privacy Assessments*** can be undertaken by and independent *Assessor* within the *Applicant's* organisation or an external appropriately qualified *Assessor.* There is currently (at time of publication) no advice for approved lists of *Privacy Assessors.*
- ***Accessibility Assessments*** involve an *assessment* against the *Web Content Accessibility Guidelines* (WCAG). There is currently (at time of publication) no advice for approved lists of *Accessibility Assessors*. *Applicant*s must deem if an *Accessibility Assessor* is appropriately qualified to conduct the assessment according to the TDIF Requirements.

Functional Assessment Process

The *Functional Assessment* process is generally conducted as follows:

1. *Applicant* engages an *Assessor* to conduct a *Functional Assessment*
2. *Assessor* conducts the *Functional Assessment* according to the relevant requirements as set out in **section 7** of the *TDIF 04 Functional Requirement*s and any other applicable requirement sections
3. *Assessor* prepares a report for the *Applicant* with the details of their *Functional Assessment* and the results
4. The *Applicant* prepares a *Functional Assessment Report* which includes:
    a. The Assessor's complete report on the *Functional Assessment*

b. The *Assessor*'s *Functional Assessment* results
c. All relevant report information as per the requirements for that type of *Functional Assessment*
d. All report information as per ASSESS-07-04-01
e. The *Accountable Executive*'s response to any risks, recommendations or non-compliances and any implementation dates for fixes. These will be added to the *Applicant*'s *Forward Work Plan*.
f. Any additional information that supports the *Functional Assessment*

5. The *Applicant* submits the *Functional Assessment Report* to *Finance*
6. *Finance* assesses the *Functional Assessment Report* and deems whether it is sufficient to meet the TDIF requirements
    a. For any recommendations, risks or non-compliances assigned a risk rating as per **Appendix A: Risk Ratings** of *TDIF 04 Functional Requirement*s and an implementation date, *Finance* will assess the *Applicant*'s risk matrix and justification of the assigned risk rating.
    b. *Applicant*s must be aware of the consequences of each risk rating as described in **Appendix A: Risk Ratings** of *TDIF 04 Functional Requirement*s.
7. Any items added to the *Applicant*'s *Forward Work Plan* will be tracked and assessed for completion on the due date.
    a. *Applicant*s must be aware of obligations regarding outstanding *Forward Work Plan* items assessed as part of their *Annual Assessment*. Further information and requirements regarding these items are located in *TDIF 07 Maintain Accreditation.*

Templates for each type of *Functional Assessment Report* are available on the *Digital Identity* website. See: Trusted Digital Identity Framework (TDIF) | Digital Identity

Alternative Assessment Reports

Finance recognises that some of the *TDIF Functional Assessments* may be equivalent to assessments an *Applicant* may have conducted on their *Identity System* prior to seeking TDIF Accreditation.

The *Applicant* may, as per its *TDIF Application Letter* and in accordance with the requirements set out in **Section 3.2.3** of *TDIF 03 Accreditation Process*, submit an *Alternative Assessment Report* and request *Finance* consider it as a substitute for a *Functional Assessment* or as evidence to meet other TDIF requirements.

PIA and Privacy Assessment

*Relates to TDIF requirements **ASSESS-07-05-01** to **ASSESS-07-05-03** of **section 7.5** in the TDIF 04 Functional Requirements.*

For guidance regarding the *Privacy Impact Assessment*, refer to **section 3.3** of the *TDIF 04 Functional Requirements* and the *Privacy Guidance* section of *TDIF 04A Functional Guidance*.

The *Privacy Assessment* is required to be undertaken as part of initial accreditation after the *Applicant* has performed a *PIA*. It is an audit of the *Applicant's Identity System* against the TDIF Privacy Requirements and must be undertaken by a qualified *Assessor.*

By the time the *Privacy Assessment* is undertaken by an *Assessor*, the following activities should be complete:

- The *Applicant* has provided *Finance* with the privacy documentation and evidence required to meet the TDIF Privacy Requirements, including the *Applicant's Privacy Policy*, a *Privacy Management Plan* and *Data Breach Response Plan*.
- An independent *Assessor* has conducted a *PIA* on the *Applicant's Identity System*.
- The *Applicant* has provided *Finance* with a *Functional Assessment Report* for the PIA, which outlines how and when they will address the recommendations outlined in the *PIA*, if any.

The *Privacy Assessment* must then be conducted according to ASSESS-07-05-03.

Templates for the *PIA* and the *Privacy Assessment Functional Assessment Reports* are available on the *Digital Identity* website. See: Trusted Digital Identity Framework (TDIF) | Digital Identity

*Privacy Assessment*s – the *OAIC* has a *Guide for undertaking privacy impact assessments.* See: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

Security Assessment and penetration test

*Relates to TDIF requirements **ASSESS-07-06-01** to **ASSESS-07-06-02** of **section 7.6** in the TDIF 04 Functional Requirements.*

Penetration Testing

Penetration Testing—also called pen testing or ethical hacking—is the practice of stress testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. *Penetration testing* can be automated with software applications or performed manually.

The *Council of Registered Ethical Security Testers* (CREST) is an international accreditation and certification body, representing and supporting the technical information security industry. CREST recognises and can award certification to organisations and *Individual*s who provide technical cyber security services such as *penetration testing*, cyber incident response capability and cyber threat intelligence.

ASSESS-07-06-01 and ASSESS-07-06-02 require *Applicant*s to engage an *Assessor* to conduct *Penetration Testing* prior to engaging a *Security Assessor* for a *Security Assessment.* This is to ensure that the requirement of ASSESS-07-06-01 for the *Security Assessment* to address the findings and recommendations from the *Penetration Testing* can be met.

Security Assessment

Security Assessments are conducted to identify any security deficiencies in the *Applicant*'s policies, processes, and *Identity System*. The *Security Assessment* must also include a review and assessment of the *Applicant*'s compliance with **Section 4** of *TDIF 04 Functional Requirement*s.

Assessments can be undertaken by a security advisor, *IRAP Assessor* or other security professional that has relevant, reasonable and adequate experience, training and qualifications to undertake the assessment. *Applicants* need to demonstrate to *Finance* how the information security *Assessor* is independent from the development and operational teams of the *Applicant's Identity System* and how there are no conflicts of interest in performing the *assessment*.

CREST can provide further information regarding *Penetration Testing* procurement. See: https://www.crest-approved.org/knowledge-sharing/implementation-procurement-guides/index.html

The *Australian Signals Directorate* publishes a list of qualified ICT security professionals that are registered under the Information Security Registered *Assessor*s Program (IRAP) to provide information security services. See: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-*Assessor*s

*Security Assessment*s – the *ACSC* has further information regarding *IRAP* assessment reporting. See: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-resources

Templates for the *Security Assessment and Penetration Test Functional Assessment Reports* are available on the *Digital Identity* website. See: Trusted Digital Identity Framework (TDIF) | Digital Identity

Accessibility assessment

*Relates to TDIF requirement **ASSESS-07-07-01** of **section 7.7** in the TDIF 04 Functional Requirements.*

The *Web Content Accessibility Guidelines* contain further information on conformance requirements in order to meet the *TDIF Accessibility Assessment*.

- For *WCAG 2.0* see: https://www.w3.org/TR/WCAG20/#conformance
- For *WCAG 2.1* see: https://www.w3.org/TR/WCAG21/#conformance .

The *How to Meet WCAG (Quick Reference)* tool developed by the W3C contains useful filters for applicable *WCAG* requirements. See: How to Meet WCAG (Quickref Reference) (w3.org)

A Template for the *Accessibility Assessment Functional Assessment Report* is available on the *Digital Identity* website. See: Trusted Digital Identity Framework (TDIF) | Digital Identity

Appendix A: Potential Sources of Risk

The following table lists potential sources of risk that should be considered by *TDIF Applicants* as part of their risk management process.

The following questions should be considered for each relevant risk:

- What is the likely outcome of the risk eventuating?
- When and how frequently can the risk happen?
- Where is the risk likely to impact?
- Who could be impacted by the occurrence of the risk event?
- What catalysts could lead to the risk event?
- How can eventuality of the risk be mitigated?
- How can the consequences of the risk event be mitigated?
- How reliable is the information that this *Risk Assessment* is being based on?

*Applicant*s should refer to *ISO 31000 Risk Management* or their own risk management framework for a description of risk, likelihood and consequence ratings.

Table 2: potential sources of risk[1]

Risk type	Potential sources of risk
Organisational risks	Supply chain (including using third party or cloud environments). Shared tenancy requirements. Lack of regular security reviews. Inadequate security *Risk Assessment* undertaken. Failure to comply with the *TDIF* accreditation requirements. Reputation damage resulting from system or compromise of *identity* information. *Identity* fraud. Known or previous cyber security incidents.
Protective security risks	Physical Security Building location, type and construction. Inadequate treatment of physical security requirements. Local crime activity. Building setbacks relative to street frontage. Pedestrian traffic. Vehicular traffic. Logical Security

[1] This list is non-exhaustive.

Risk type	Potential sources of risk
	Inappropriate storage of *ICT* and information assets. Use of non-evaluated *ICT* assets. *ICT* asset failures. *Relying Party ICT* asset failures. Malicious code or ransomware infection. Exploitation through security vulnerabilities. Denials of service. Unauthorised access to systems. Data spills. Potential for error (e.g. system error, processing error, internal user error, etc). Source of data and nature of data entry. Extent and nature of system or application change. Network environment and structure. System integration failures. Fire or flood. Location and security of environments used to support the *Applicant's* operations. Poor disaster recovery and business continuity planning. Availability and redundancy of entry points for communications services and essential services. Internet connectivity outages. Long term electricity outages.

Risk type	Potential sources of risk
	Personnel Security Personal harm to *Individuals* that use the *identity* service. Inadequate *personnel* security checks undertaken. Inadequate security awareness training provided. Abuse of privileges by internal staff or administrators.
Identity risks	Falsified *identity documents* used during *identity proofing*. Fraudulent use of another's *identity*. An *Individual* denies *proofing*, claiming it wasn't them. Overlapping *identity*, e.g. two *Individuals* or more associated with one *identity* Incorrect attribution of *identity*, e.g. an *Individual* associated with another's *identity*, or source records that are mixed and don't separate unique *Individuals*. Social engineering on an *Individual* for their *identity* information. *Identity Service Provider* unable to verify *identity* information at source, due to unavailability, incorrect or inconstant source data. E.g. Name is misspelt in some records; records not available. Legitimate *user* unable to prove or assert *identity*, particularly in a timely manner: at initial proofing, or after their *identity* is misused. Unintended disclosure of *identity* information to a third party. Compromise of *identity* information by *Identity Service Provider* (trusted insider) or *attacker* (malicious outsider).

Risk type	Potential sources of risk
Authentication credential risks	Unintended disclosure of *credential* to third party. Unauthorised duplication or reproduction of *credential.* *Credential* compromised through modification or tampering. *Credentials* insecure against brute force attacks. *Credentials* insecure against offline attacks. *Cryptographic-based credentials* use unsupported algorithms. Inability of *Credential Service Provider* to suspend or revoke *credentials*. Incorrect *credential* suspended or revoked. Inability of *Credential Service Provider* to recover lost *credentials*. Inability of *Credential Service Provider* to renew or issue a replacement *credential*. Incorrect *credential* renewed, recovered or replaced. Unauthorised issuance of *credentials* to third party. Social engineering of *Individual* for their *credential*. *Credentials* are not unique or not uniquely identifiable. Risks associated with device swap, SIM change, number porting or other abnormal behaviour
Authenticated session risks	Insecure transfer of *identity attributes, assertions* and *credentials* between *Accredited Providers.* Inability to measure normal and legitimate *authentication* behaviours. Inability to detect or report abnormal *authentication* behaviours.

Risk type	Potential sources of risk
	Suspended or revoked *credentials* are accepted by *Accredited Providers.* Unsupported or insecure cryptographic algorithms or protocols are used to secure information transfers between *Accredited Providers.* Insecure against replay attacks (see: *replay resistance*). Insecure against *Man-in-the-Middle* or *Man-in-the-Browser* attacks.
Downstream	*Individuals* obtaining services or payments that they are not entitled to. Refusal of services for legitimate claimants.