Australian Government

Digital Identity

04A Functional Guidance

Trusted Digital Identity Framework

Release 4 June 2021, version 1.2

PUBLISHED VERSION

Digital Transformation Agency (DTA)

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

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

Document management

The DTA has reviewed and endorsed this document for release.

Change log

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	May 2020		Published version
1.1	Feb 2021	JK	CRID0004 – Biometrics guidance changes, major style, format, grammar and referencing changes. CRID0013 – Templates updated and now available on website
1.2	June 2021	JK, MS	CRID0009 - Added Digital Identity Risk Management guidance, additional privacy guidance

All changes made to the TDIF are published in the TDIF Change Log which is available at https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework.

Contents

Introduction

This document provides guidance to *Applicants* undergoing the *TDIF Accreditation Process* on how to meet the *TDIF 04 - Functional Requirements.* Over time this document will be updated with specific guidance for meeting *TDIF* requirements and how the DTA will assess compliance. This document includes guidance on:

- Fraud Control.
- Privacy.
- Protective Security.
- User Experience.
- *Technical testing*.
- *Functional assessment*s.

The intended audience for this document includes:

- Accredited *Provider*s.
- *Applicant*s.
- Assessors.
- 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 and implementation of an Applicant's *identity system* must be informed by an assessment of the risks associated with operation of their digital identity system.

Risk assessments 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 as a component of broader fraud, privacy and information security risk assessments. For *TDIF Applicants,* risk management activities are linked to the following requirements:

- Section 2 of the *TDIF 04 Functional Requirements* sets out the requirements for *Applicants* to implement *Fraud Control Plans* and manage fraud-related risks.

- Section 3.2 and 3.3 of the *TDIF 04 Functional Requirements* sets out the requirements for *Applicants* to implement effective privacy governance, including requirements to establish privacy roles, implement *Privacy Management Plans*, policies and undergo *Privacy Impact Assessments* to identify and minimise privacy related risks.

- Section 4.1.3 of the *TDIF 04 Functional Requirements* sets out the requirements for Applicants to implement System Security Plans and undergo security risk assessments.

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 management activities.

Risk assessments should consider the impacts to the organisation itself, as well as the risks associated with the misuse of any resulting *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 difficulties 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.

- **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 System***: 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 also consider non-*identity proofing* risk mitigation strategies. 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). These mitigation strategies may provide a more cost-effective option to counter *digital identity* fraud than rigorous *identity proofing* processes. 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*).

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 being applicable to the *Applicant*.

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

Accountable Authority

Relates to TDIF requirements ***FRAUD-02-01-01*** *to* ***FRAUD-02-01-03*** *of section* ***2.1*** *in the TDIF 04 Functional Requirements.*

Part 4 of the *CFCF* will guide *Applicants* on the responsibilities and accountability for fraud control arrangements.

The *Public Governance, Performance and Accountability Act 2013* (PGPA Act) states that the *Accountable Authority* must govern the entity in a way that promotes:

- the proper use and management of public resources.
- the achievement of the purposes of the entity.
- the financial sustainability of the entity.

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* will guide *Applicants* on *Fraud Control Plans*.

A template for the Fraud Control Plan is available from the *DTA* website. See: https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework

Fraud Prevention, Awareness and Training

*Relates to TDIF requirements **FRAUD-02-03-01** to **FRAUD-02-03-07** of section **2.3** in the TDIF 04 Functional Requirements.*

Part 7 of the *CFCF* will guide *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)

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* will guide *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-02-05-10b** of section **2.5** in the TDIF 04 Functional Requirements.*

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

Support for victims of identity fraud

*Relates to TDIF requirements **FRAUD-02-06-01** to **FRAUD-02-06-05** of section **2.6** in the TDIF 04 Functional Requirements.*

Applicants should consider leveraging the following resources:

- 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 individuals 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-03-01-03** 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 Requirements and Guidance documents of *TDIF.* 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/

Where an Applicant is required to opt-in to the coverage of the *Privacy Act 1988* (Cth), this involves a formal process by which the *Applicant* must complete the application form and provide 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

*Relates to TDIF requirements **PRIV-03-02-01** to **PRIV-03-02-09** of section **3.2** in the TDIF 04 Functional Requirements.*

The privacy assessment is required after the *Applicant* has performed a *Privacy Impact Assessment.* Essentially, a *privacy assessment* is an assessment against the *TDIF* requirements, completed by an *assessor,* and submitted as evidence to the *DTA* to address the *Privacy Requirements*.

A template for the *Privacy Assessment* and the *Privacy Impact Assessment* is available on the DTA website. See: https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework

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* to understand and perform 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.

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 may help staff understand their responsibilities and avoid practices that would breach privacy obligations. Training should consider new starters, contractors and temporary staff.

Applicants and their staff should understand the importance of good information handling practices and 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-03-03-01a** of section **3.3** in the TDIF 04 Functional Requirements.*

A *PIA* needs to be conducted for all high privacy risk projects related to an *Applicant's* identity system. A project may be a high-risk project if the *Applicant* reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of *individual*s.

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 the required *PIA* is available on the *DTA* website. See: https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework

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.*

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/assets/privacy/guidance-and-advice/data-breach-preparation-and-response.pdf.

Notification of Collection

*Relates to TDIF requirement **PRIV-03-05-01** 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.*

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 as sensitive information in the *Privacy Act 1988* and includes *biometric information* that is to be used for the purpose of automated *biometric verification* or biometric identification or biometric templates. *Sensitive information* can only be collected with the explicit consent of the *individual*.

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/

Consent

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

Consent means *Express Consent* or *Implied Consent*. Guidance on *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 the operation of a part of its business covered by the *TDIF* are required to provide evidence to the *DTA* 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/

Government Identifiers

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

A government related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract.

Where an identifier, including a government related identifier, is *personal information*, it must be handled in accordance with the Australian Privacy Principles[1].

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

Access, correction and individual history log

*Relates to TDIF requirements **PRIV-03-12-01** to **PRIV-03-12-08** of section **3.12** in the TDIF 04 Functional Requirements.*

Guidance 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/

1 Or equivalent principles and regulations in other jurisdictions.

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).

Included in the requirement is that *Applicants* should not re-identify data through public or other sources and must take reasonable steps to ensure this does not occur accidentally or that data passed to third parties cannot re-identify *individual*s.

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

Several requirements listed in the *TDIF 04 Functional Requirements* 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*). These requirements ensure *Applicants* establish a minimum protective security baseline for their identity service.

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*.
- References to *PSPF*, *AGIS* or *ISM* controls that are applicable to an agency are to be interpreted as being applicable to the *Applicant*.
- The scope of *PSPF*, *AGIS* or ISM controls are limited to the identity service 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.

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.

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 TDIF requirements **PROT-04-01-01** to **PROT-04-01-19a** of section **4.1** in the TDIF 04 Functional Requirements.*

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

Role of the Accountable Authority

*Relates to TDIF requirements **PROT-04-01-01** to **PROT-04-01-03** of section **4.1.1** in the TDIF 04 Functional Requirements.*

The *PSPF GOVSEC-01 (Role of the Accountable Authority)* describes the role and responsibilities of the *Accountable Authority.* 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/sites/default/files/pspf-govsec-01-role-accountable-authority.pdf

Management structures and responsibilities

*Relates to TDIF requirements **PROT-04-01-04** to **PROT-04-01-11** of section **4.1.2** in the TDIF 04 Functional Requirements.*

The *PSPF GOVSEC-02 (Management structures and responsibilities)* describes 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/sites/default/files/pspf-govsec-02-management-structures-responsibilities.pdf

Security risk assessments

*Relates to TDIF requirements **PROT-04-01-12** to **PROT-04-01-18** of section **4.1.3** in the TDIF 04 Functional Requirements.*

The *PSPF GOVSEC-03 (Security planning and risk management)* guide *Applicants* in 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/sites/default/files/pspf-govsec-03-security-planning-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 will guide *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/sites/default/files/pspf-govsec-04-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)* describes how *Applicants* are required to detail how they 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/sites/default/files/2019-11/pspf-infosec-08-sensitive-classified-information.pdf

Access to information

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

The *PSPF INFOSEC-09 (Access to Information)* details the 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/sites/default/files/2019-11/pspf-infosec-09-access-information.pdf

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* mitigate common and emerging cyber threats, which may include:

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

The most common cyber threat facing *Applicants* is external adversaries who attempt to steal data. Often these adversaries 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. The *Essential Eight* represents the best advice on the measure *Applicants* can implement to mitigate cyber threats.

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 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-04-02-16** of section **4.2.4** in the TDIF 04 Functional Requirements.*

The Australian Cyber Security Centre has developed prioritised mitigation strategies to help organisations mitigate cyber security incidents caused by various cyber threats. The mitigation strategies are known as the *Essential Eight*.

While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline, the *Essential Eight*, 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.

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

Further information on strategies to mitigate cyber security incidents is available from the *ACSC*. See: https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

Robust ICT Systems

*Relates to TDIF requirements **PROT-04-02-21** to **PROT-04-02-25** of section **4.2.6** in the TDIF 04 Functional Requirements.*

The *PSPF INFOSEC-11 (Robust ICT systems)* details 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/sites/default/files/pspf-infosec-11-robust-ict-systems.pdf

Disaster recovery and business continuity management

*Relates to TDIF requirements **PROT-04-02-26** and **PROT-04-02-27** 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-04-02-28** to **PROT-04-02-29** 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*):

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/privacy-and-security/trusted-digital-identity-framework

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)* describes 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/sites/default/files/pspf-persec-12-eligibility-suitability-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)* details 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:

- 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/sites/default/files/pspf-persec-13-ongoing-assessment-personnel.pdf

Separating personnel

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

The *PSPF PERSEC-14 (Separating personnel)* details the 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/sites/default/files/pspf-persec-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)* details 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/sites/default/files/pspf-physec-15-physical-security-entity-resources.pdf

User Experience Guidance

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

The *User* experience needs be shaped and positioned into 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.

Sources:

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

The *W3C* website has further information and guidance. 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.*

Usability is part of the broader term “user experience” and focuses on how easy user interfaces are used to achieve the intended outcome.

ISO 9241-210 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* find and consume content. Only design and write content that meets a real person’s need and write content to an Australian year 7 level

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

The DTA *Digital Service Standard* provides further usability guidance. See: https://www.dta.gov.au/help-and-advice/build-and-improve-services/service-design-and-delivery-process/own-whole-user-experience

Identity verification journey and authentication journey

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

Ensuring users are as prepared as possible to use the identity service is critical to the overall success and usability of an identity service. To meet the *TDIF* requirements for the identity verification journey, *Applicants* should provide upfront information that assists *Users* to follow the process simply and safely including:

- Technical requirements such as internet access and a webcam
- Identity document requirements
- Useful feedback throughout 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.*

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.

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

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

This section provides guidance for the testing processes that are implemented to run an effective technical testing program. Requirements **FED-02-01-05** and **FED-02-02-01** in *TDIF: 06 – Federation Onboarding Requirements* also require that an *Applicant* conduct *Technical testing* in accordance with section 6 of the *TDIF: 04 - Functional Requirements*.

This guidance is applicable to:

- Major Changes – the development of new or changed functionality to implement substantial changes to the system
- Enhancement – the development of new or changed functionality to an existing system without substantially changing the system, including minor upgrades.
- Defect – corrections to the existing system where the system does not meet its defined and approved functionality and requires modification.

The test process is considered to comprise of the following:

- Planning.
- Execution of Testing.
- Test Completion.

A template for the *Technical Test Plan* and the *Technical Test Report* is available on the *DTA* website. See: https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework

Technical Test Planning

*Relates to TDIF requirements **TEST-06-01-01** to **TEST-06-01-08** of section **6.1** in the TDIF 04 Functional Requirements.*

Prior to undertaking testing, the *Applicant* is required to develop a *Technical Test Plan* and provide it to the *DTA*. This is intended to give the *DTA* visibility of the processes used by the *Applicant* to test the technical requirements against their system. Apart from the test completion criteria, the individual components of the

Technical Test Plan do not need to be agreed upon with the *DTA*; however, the *DTA* may raise any concerns they have with its contents with the *Applicant*.

Test completion criteria refers to the criteria which the results of the test execution will be measured against. This may include criteria regarding the pass rates and the execution coverage. An example of test completion 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.

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.

Technical Testing

*Relates to TDIF requirement **TEST-06-02-01** and **TEST-06-02-02** of section **6.2** in the TDIF 04 Functional Requirements.*

Technical Testing involves the execution of the test cases developed as part of the *Applicant's Technical Test Plan* and the comparison of the expected results against the actual results. During this phase defects should be identified, resolved and retested. These defects, if not dealt with during testing, will be considered by the *DTA* during evaluation of the *Technical Test Report*.

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 execution coverage as well as the status for each test case and must be included in the *Technical Test Report*.

Technical test completion

*Relates to TDIF requirements **TEST-06-03-01** to **TEST-06-03-02** of section **6.3** in the TDIF 04 Functional Requirements.*

The *Applicant* must submit a *Technical Test Report* that demonstrates the *Technical Testing* of their system has been executed in accordance with the approved *Technical Test Plan.*

The *Technical Test Report* should include:

- An outline of the status of all test cases, including the execution coverage and defects
- The test completion criteria, for criteria that have been met
- A risk assessment against criteria that have not been met during *Technical Testing*.

Functional Assessments Guidance

*Relates to TDIF requirements **ASSESS-07-01-01** to **ASSESS-07-07-03** of section **7** in the TDIF 04 Functional Requirements.*

Sources:

- Privacy assessments – 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 assessments – the *ACSC* has further information regarding *IRAP* assessment reporting. See: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-resources
- *Accessibility* – the *Web Content Accessibility Guidelines* contains further information on conformance requirements.
    - For *WCAG 2.0* see: https://www.w3.org/TR/WCAG20/#conformance
    - For *WCAG 2.1* see: https://www.w3.org/TR/WCAG21/#conformance

Templates for Functional Assessments are available on the *DTA* website. See: https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework

PIA and Privacy Assessment

*Relates to TDIF requirements **ASSESS-07-01-01** to **ASSESS-07-01-04** of section **7.1** in the TDIF 04 Functional Requirements.*

For guidance regarding the Refer to section 3.3 *Privacy Impact Assessment* of the *TDIF: 04 - Functional Requirements* and the *Privacy Guidance* section of *TDIF 04A – Functional Guidance*.

The *privacy assessment* is required after the *Applicant* has performed a *PIA*. It is an audit of the *Applicant's* system against the TDIF Privacy Requirements and must be undertaken by a qualified *Assessor.*

The aim of the *privacy assessment* is to:

- Determine whether the *Applicant* can demonstrate it has complied with the Privacy Requirements.
- Determine whether the *Applicant* has addressed all recommendations arising from the PIA.
- Document the results of the *privacy assessment* in a report to the *DTA*.

The following activities have occurred by the time the *privacy assessment* is undertaken:

- The *Applicant* has provided the *DTA* with a plan demonstrating how they will meet the Privacy Requirements.
- The *Applicant* has provided the *DTA* with required privacy documentation, including a *Privacy Management Plan* and *Data Breach Response Plan*.
- An independent assessor has conducted a *PIA* on the *Applicant*.
- The *Applicant* has provided the *DTA* with a report which outlines how and by when they will address the recommendations outlined in the *PIA* (this should be submitted with the *PIA*).
- The *Applicant* has submitted protective security, risk management and fraud control documentation to the *DTA*. This provides additional context to the *privacy assessment*.

Templates for the *PIA* and the *privacy assessment* are available on the *DTA* website. See: https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework

Security Assessment and penetration test

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

Penetration testing, also called pen testing or ethical hacking, is the practice of 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 individuals who provide technical cyber security services such as *penetration testing*, cyber incident response capability and cyber threat intelligence.

It is recommended to complete *Penetration Testing* prior to engaging a *Security Assessor.* This is because the *Security Assessor* is able to assess the *Penetration Test* results and provide advice and interpretation to better calculate security risks to the *Applicant's* system.

Security assessments are undertaken on an *Applicant's* identity service against the *TDIF* protective security requirements. *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. Further, *Applicants* need to demonstrate to the *DTA* 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 Assessors Program (IRAP) to provide information security services. See: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors

Accessibility assessment

*Relates to TDIF requirement **ASSESS-07-03-01** of section **7.3** in the TDIF 04 Functional Requirements.*

Refer Section 5.6 *Accessibility requirements of 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

Applicant obligations

*Relates to TDIF requirements **ASSESS-07-04-01** and **ASSESS-07-04-02** of section **7.4** in the TDIF 04 Functional Requirements.*

Applicants define the scope, objectives and criteria for the following *Functional Assessments*:

- *Privacy Impact Assessment.*
- *Privacy assessment.*
- *Security assessment.*
- *Penetration test.*
- *Accessibility assessment.*

Assessor skills, experience and independence

*Relates to TDIF requirements **ASSESS-07-05-01** and **ASSESS-07-05-02** of section **7.5** in the TDIF 04 Functional Requirements.*

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

There is currently (at time of publication) no advice for approved lists of *Privacy Assessors* or *Accessibility Assessors*. *Applicants* should present evidence of the ***Assessor's*** skills, experience, qualifications and independence when engaging an *assessor* for a *Privacy* or *Accessibility assessment*.

Functional Assessment Report

*Relates to TDIF requirements **ASSESS-07-07-01** to **ASSESS-07-07-03** of section **7.7** in the TDIF 04 Functional Requirements.*

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

The *Functional Assessment* reports must use the following compliance ratings from *Appendix A* in *TDIF 04 Functional Requirements*:

Refer to the *ISO 31000* or the *Applicant's* own risk management framework for a description of likelihood and consequence ratings.

- **Not Applicable (N/A).** A *TDIF* requirement that does not apply to an *Applicant* as their identity system does not use, rely on or support the *TDIF* requirement (for example, *TDIF* requirements for elliptic curve cryptography will be N/A if the identity system supports other *AACAs* instead).
- **Compliant.** The *Applicant* has demonstrated with evidence they comply with a *TDIF* requirement or the intent of a requirement.
- **Critical Non-Compliance.** The *Applicant* fails to meet a *TDIF* requirement which may result in extreme unmitigated risk.
    - A critical non-compliance must be classified as a critical failure and must result in a failed *Functional Assessment.*
    - The immediate withdrawal of an existing accreditation may occur until such time as the critical non-conformance is addressed.
- **Major Non-Compliance**. The *Applicant* fails to meet a *TDIF* requirement which may result in high unmitigated risk.
    - A major non-compliance must be classified as a major failure and must result in a failed *Functional Assessment*.

- Escalation of the problem to a critical failure must be imposed if additional events impact on the *Applicant* simultaneously.
- If the *Applicant* fails to rectify the compliance problem within a timeframe agreed with the *DTA*, then the status of the problem must be escalated to a critical failure and the conditions of that category are then applied.

- **Partial Non-Compliance.** The *Applicant* fails to meet a *TDIF* requirement which may result in moderate unmitigated risk must be classified as a partial failure.
  - Escalation of the problem to a major failure must be imposed if additional failures within this category are detected.
  - If the *Applicant* fails to rectify the compliance problem within a timeframe agreed with the *DTA*, then the status of the problem must be escalated to a major failure and the conditions of that category are then applied.
- **Minor Non-Compliance.** The *Applicant* fails to meet a *TDIF* requirement which may result in low unmitigated risk should be classified as minor failures.
  - Escalation of the problem to a partial failure must be imposed if additional failures within this category are detected.
  - If the *Applicant* fails to rectify the compliance problem within a timeframe agreed with the *DTA*, then the status of the problem must be escalated to a partial failure where the conditions of that category are then applied.

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 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?
- Who are the stakeholders of the risk event? What is the impact on them?
- 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?

Table 2: potential sources of risk[2]

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

[2] 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.