Australian Government
Digital Transformation Agency

Protective Security Reviews

Trusted Digital Identity Framework
August 2018, version 1.03

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Conventions

The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" in this document are to be interpreted as described in the current version of the *Trusted Digital Identity Framework: Overview and Glossary*.

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you have difficulties accessing this document, or have questions or comments regarding this document please email the Director, Trusted Digital Identity Framework at identity@dta.gov.au.

Document Management

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

Change log

Version	Date	Author	Description of the changes
0.01	Jan 2017	SJP	Initial version
0.02	May 2017	SJP	Updated content to align with current editions of the ISM and PSPF. Migrated information to the current DTA template.
0.03	Jul 2017	SJP	Minor updates to align with other Trust Framework documents
0.04	Sept 2017	SJP	Minor updates to support the public consultation draft
0.05	Jan 2018	SJP	Incorporates feedback from stakeholders and public consultation. Relabelled the document to Protective Security Reviews to accommodate penetration testing in the next edition.
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority
1.01	Feb 2018	TC, CD & EF	Initial draft of penetration testing requirements
1.02	Mar 2018	HWC	Penetration testing and vulnerability management updates
1.03	Aug 2018	SJP	Updated to incorporate stakeholder feedback

Contents

1 Introduction

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

Applicants that apply for accreditation under the TDIF undergo rigorous evaluations of all aspects of their operations, including compliance with applicable Unclassified Australian Government protective security requirements as outlined in the current editions of the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM). In support of these compliance obligations, this document outlines the protective security reviews to be performed on an Applicant's identity service as defined in the *TDIF: Protective Security Requirements*.

This document includes two parts

- Part one: defines the Information Security Registered Assessors Program (IRAP) Assessment – the roles, responsibilities, process and expected outcome.
- Part two: defines the security testing requirements covering vulnerability management and penetration testing.

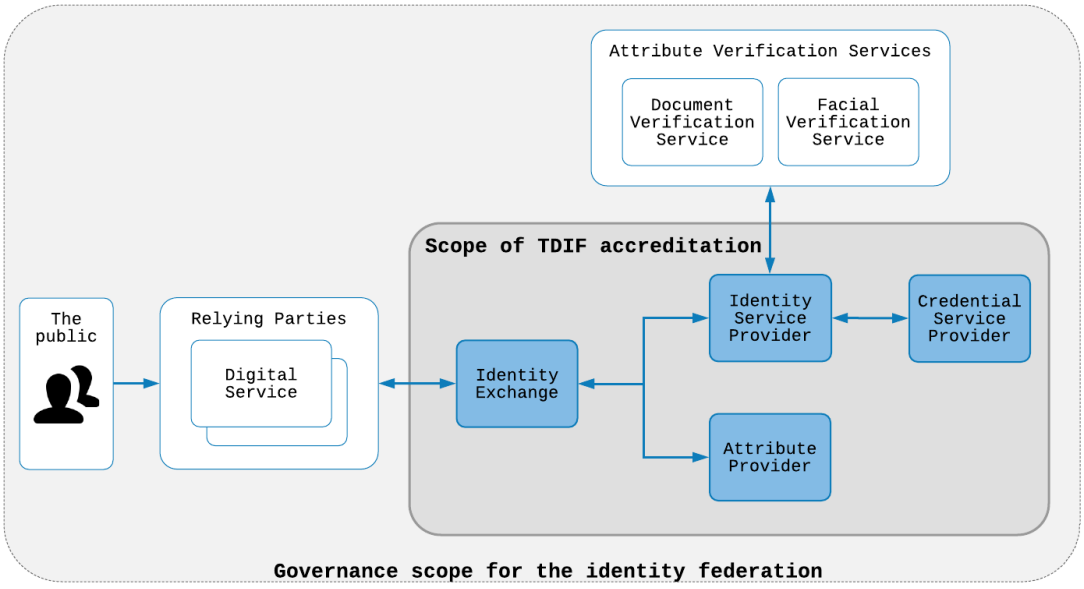
The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Authorised Assessors (in the context of this document that means IRAP Assessors, vulnerability assessors and penetration testers).
- Australian Signals Directorate (ASD).
- Information security practitioners.
- Relying Parties.
- Trust Framework Accreditation Authority.

1.1 Overview

The digital identity federation relies on each component system maintaining high levels of assurance and trustworthiness. A compromise in the confidentiality, integrity or availability of a component of the federation could significantly impact trust in the end-to-end service. Security testing is required in order to validate that security controls are working effectively. It is a core component of the overall TDIF assurance and accreditation process.

Figure 1: – components of the federated digital identity system.



Each of the components detailed in Figure 1 operate under the TDIF and as such are assured individually and as a whole.

2 IRAP assessment

2.1 Roles and responsibilities

2.1.1 Applicant

The Applicant is responsible for:

- Preparing all required protective security documentation.
- Retaining the services of an independent IRAP Assessor to perform the IRAP assessment. The Applicant, at its discretion, can request the IRAP Assessor sign a confidentiality or non-disclosure agreement prior to performing the IRAP assessment.
- Supporting the IRAP Assessor as required during the assessment.
- Remediating all identified non-compliance issues to the satisfaction of the Trust Framework Accreditation Authority.

2.1.2 IRAP Assessors

IRAP Assessors are responsible for:

- Undertaking an evaluation on the identity service in accordance with the Statement of Applicability[1].
- Documenting the results of the IRAP assessment in a Findings Report which:
    - Summarises the activities performed during the IRAP assessment.
    - Suggests remediation actions to address non-compliance.
    - Recommending whether or not the Applicant has satisfied the requirements of this document.

2.1.3 Trust Framework Accreditation Authority

The Trust Framework Accreditation Authority is responsible for:

[1] See section 2.4.1 for further details

- Ensuring that the Trust Framework Accreditation Process is conducted with due care and in accordance with the published Trust Framework documents.
- As appropriate, accepting (or rejecting) Applicant's existing waivers against ISM or PSPF.
- Reviewing Findings Reports and considering the recommendations.
- Notifying Applicants of any non-compliance issues, required mitigation actions and timeframes in which to undertake the mitigation actions.
- All decisions in relation to the suitability of Applicants to continue through the Trust Framework Accreditation Process.
- Assessing the residual risk relating to the operation of the Applicant's identity service within the broader identity federation.

2.2 What is IRAP?

The IRAP is an ASD initiative to provide high-quality information and communications technology (ICT) security assessment services to government.

The ASD endorses suitably-qualified ICT professionals to provide relevant security services which aim to secure broader industry and Australian Government information and associated systems.

IRAP Assessors assist in securing computer networks by accessing information security compliance, suggest mitigations and highlighting residual risks.

2.3 IRAP Assessors

IRAP Assessors are ASD certified information security professionals endorsed to provide information security services to government. IRAP Assessors have:

- The necessary skills, experience and qualifications in information security, auditing and risk management.
- A detailed knowledge of current Australian Government information security compliance requirements.

The list of currently accredited IRAP Assessors is available on the ASD website (http://www.asd.gov.au/infosec/irap/assessors.htm). The Applicant can use anyone from the list to carry out their IRAP assessment, provided:

- The IRAP assessor is independent from the identity service being assessed.
- There are no conflicts of interest between the IRAP Assessor and the Applicant's agency or organisation.

Note: The costs associated with the IRAP assessment are to be met by the Applicant.

The cost of an IRAP assessment can vary from one IRAP Assessor to another and range between tens of thousands to a hundred thousand dollars. This cost will largely depend on the scope and timeliness of the evaluation to be performed and the maturity of the identity service being assessed. Applicants **SHOULD** contact several IRAP Assessors to get a sense of the cost, duration and complexity of the assessment prior to engaging an IRAP Assessor.

2.4 IRAP assessments

For the purpose of Trust Framework accreditation, an IRAP assessment is a review by an IRAP Assessor of the implementation, appropriateness and effectiveness of the protective security controls applied to the Applicant's identity service. The minimum protective security controls to be reviewed are defined in the *TDIF: Protective Security Requirements*.

An IRAP assessment is achieved through a two-stage evaluation which encompasses documentation reviews, a site visit and interviews with key security personnel. The outcome of the IRAP assessment is a Findings Report which is sent by the IRAP Assessor to the Trust Framework Accreditation Authority for consideration as part of the Trust Framework Accreditation Process.

The Applicant **MAY** choose to complete the IRAP assessment:

- Using one IRAP Assessor for both stages as one continuous activity (Stage One and Stage Two together).
- Using one IRAP Assessor for both stages as two separate activities (Stage One, then Stage Two at a later time), or

- Using different IRAP Assessors for Stage One and Stage Two of the assessment.

The Applicant **MUST** advise the Trust Framework Accreditation Authority which IRAP Assessor(s) it intends to use prior to commencing the IRAP Assessment.

Pre-assessment tip

- Before engaging an IRAP Assessor, conduct a self-assessment of the identity service against the *TDIF: Protective Security Requirements*. This will allow you to understand your own compliance and resolve or mitigate any non-compliance.
- Before the assessment, update the network security documentation suite. This will enable the IRAP Assessor to focus on compliance rather than identifying errors in your documentation.
- Understand the scope of the identity service you want assessed, and clearly articulate a statement of work in the contract with an IRAP Assessor.
- Do not define or expect favourable outcomes, as it can undermine the integrity of the assessment.

2.4.1 Stage One evaluation

- During stage one of an IRAP assessment, the IRAP Assessor performs the following activities:
- Defines the scope of the evaluation to be performed (referred to as the 'Statement of Applicability') in consultation with the Applicant[2].

The Statement of Applicability for the evaluation to be performed **MUST** include the identity service being assessed and how the Applicant has applied the following requirements to it:

- *TDIF: Protective Security Requirements*.
- *TDIF: Risk Management Requirements*.
- *TDIF: Fraud Control Requirements*.

The IRAP Assessor **MUST** determine whether the identity service to be evaluated is operational or not.

[2] As part of defining the Statement of Applicability, the IRAP Assessor may consider previous IRAP Assessments or other audit work (e.g. PCI-DSS) performed on the identity service in the previous twelve-month period.

- If key elements of the Applicant's identity service are not yet operational but would have been considered within the Statement of Applicability if they were operational, the IRAP Assessor **MUST**:
  - note these elements in the Findings Report.
  - recommend these elements be subject to review as part of the Applicant's annual compliance audit.
  - Such determinations **MUST NOT** adversely impact the outcome of the IRAP assessment.
- Gains an understanding of the Applicant's identity service.
- Reviews identity service architecture and supporting protective security documentation.
- Seeks evidence of compliance with Australian Government protective security policy requirements and recommendations.
- Highlights the effectiveness of protective security controls and recommends actions to address or otherwise mitigate non-compliance.
- Compliance ratings and a template for reporting compliance are located at Annex A and Annex B respectively.

The outcome of the Stage one evaluation is a draft Findings Report which is used as an input for the second stage of the evaluation.

2.4.2 Stage Two evaluation

During stage two of an IRAP assessment, the IRAP Assessor looks deeper into the operation of the identity service. The IRAP Assessor will conduct a site visit where they will:

- Conduct interviews with key security personnel.
- Investigate the implementation and effectiveness of the protective security controls with reference to the supporting protective security documentation.
- Verify consistency between the protective security documentation and operational protective security controls.
- have the Applicant demonstrate the protective security controls work as intended.
- Recommend actions to address or otherwise mitigate non-compliance.

The outcome of the second stage evaluation is a detailed Findings Report.

2.5 Protective security documentation to be reviewed

The *TDIF: Protective Security Requirements* describes the protective security documentation that Applicants are required to develop and maintain. In summary, this includes:

- Information Security Policy.
- Security Risk Management Plan.
- Vulnerability Management Plan.
- Incident Response Plan.
- Physical and Environmental Security Plan.
- System Security Plan.
- Standard Operating Procedures.
- Personnel Security Plan.
- Disaster Recovery and Business Continuity Plan.
- Emergency Response Management Procedures.
- Cryptographic Key Management Plan.

Each of these documents **MUST** be reviewed by the IRAP Assessor as part of the Stage One evaluation.

The IRAP Assessor **MUST** mark the Applicant as non-compliant if any of these documents:

- Do not include the mandatory content as per the *TDIF: Protective Security Requirements (Part two: Protective security documentation)*.
- Do not include the date, version history or it is unclear who approved their release.

2.6 Failed evaluations

A failed evaluation is one where the IRAP Assessor determines that the Applicant's implementation of its protective security policies and procedures, either:

- Does not adequately mitigate the threats, vulnerabilities and risks identified in its protective security documentation.
- Does not adequately satisfy the *TDIF: Protective Security Requirements*.

In reaching this decision the IRAP Assessor **MUST** have due regard to the nature of the Applicant's identity service, operating protective security controls, its business needs, threat environment and risk appetite. This decision is not subject to negotiation with the Applicant or the Trust Framework Accreditation Authority.

2.7 Findings Report

At the completion of stage two of the evaluation, the IRAP Assessor **MUST** prepare a Findings Report based on the activities they have undertaken in completing the IRAP assessment.

At a minimum the Findings Report **MUST**:

- Make an assessment of compliance against the requirements of this document.
- Provide a recommendation to the Trust Framework Accreditation Authority whether or not the Applicant's identity service has satisfied the *TDIF: Protective Security Requirements*.
- Include a list of compliant and non-compliant controls.
- Suggest remediation actions to address or otherwise mitigate non-compliant controls.
- Where a failed evaluation has occurred, the Findings Report **MUST** recommend the remedial action to be undertaken by the Applicant and the timeframe within which the actions are to be completed to address the non-compliance.

The IRAP Assessor **MUST** provide a copy of the Findings Report to the Applicant and the Trust Framework Accreditation Authority. The contact information of the Trust Framework Accreditation Authority is located at the top of this document.

The Trust Framework Accreditation Authority will use the Findings Report to:

- Assess the residual risk relating to the operation of the Applicant's identity service.
- Consider any remediation activities recommended by the IRAP Assessor.
- Determine whether the Applicant has satisfied the requirements of this document and is therefore suitable to continue through the Trust Framework Accreditation Process.

- The Trust Framework Accreditation Authority, may and at its sole discretion, notify other members of the identity federation when a failed evaluation has occurred.

2.8 When additional security reviews may be required

Once the Trust Framework Accreditation Authority grants accreditation to an Applicant they become an Accredited Provider of the identity federation. Other than meeting annual compliance obligations, an Accredited Provider **MAY** be directed by the Trust Framework Accreditation Authority to undergo additional security reviews. This will occur if the Accredited Provider's identity service is changed in a manner that may result in:

- Significant impacts to the Accredited Provider's protective security arrangements.
- Material changes the Accredited Provider's risk exposure.
- Material changes to the risk exposure of other participants in the identity federation.

Additional security reviews **MAY** include IRAP assessments, penetration testing, vulnerability assessments or security risk assessments. In such circumstances, the Trust Framework Accreditation Authority will advise the Accredited Provider in writing of the requirement for them to undergo one or more additional security reviews. The costs associated with these activities **MUST** be met by the Accredited Provider and **MUST NOT** replace their annual compliance obligations.

3 Security testing requirements

3.1 Vulnerability management

Objective: Vulnerabilities within systems are identified, assessed and mitigated on an ongoing basis over time.

Rationale: Maintaining the security of a system is a continual process that extends beyond ensuring it is secure at the time of deployment. Vulnerabilities can be introduced into a system during development, implementation, change management, changes in technology, attack vectors and the threat environment. Vulnerabilities, if unmitigated, provide an avenue for a malicious party to compromise systems and information.

Requirement:

The Applicant **MUST** as a minimum:

- Document and implement a Vulnerability Management Plan to detect and mitigate security vulnerabilities within the environment.
- Undertake a vulnerability assessment on systems before they are deployed into operation and on an ongoing once a system is deployed

3.2 Penetration testing

Objective:

1. The strength and effectiveness of security controls are tested on an ongoing basis over time.
2. Control weaknesses are identified and remediated in a prompt and proactive manner.
3. Evidence of testing and test outcomes is recorded and retained as part of the assurance and accreditation process.

Rationale: penetration testing, tests the actual or real-world effectiveness of implemented security controls against attack. It seeks to replicate the types of actions that a malicious attacker would take, therefore giving a more accurate representation of the security posture of the environment at any given time.

Penetration testing is complimentary to a vulnerability management process in that it also tests for weaknesses in system interactions and validates the existence of vulnerabilities through exploitation.

Requirement:

The Applicant **MUST** as a minimum:

- Conduct penetration testing:
  - Prior to systems being deployed into operation.
  - Annually, once systems have been deployed into operation.
  - When there is a substantial change in their structure, technical capability, functions or activities.
  - When determined necessary by protective security personnel.
- Undertake application code reviews for non-COTS products as part of the software development process.
- Penetration testing and application code reviews must be undertaken by protective security specialists who are independent from the development team. Protective security specialists can either be internal staff or third parties.
- Document a Penetration Testing Plan which clearly articulates the scope of tests to be conducted, constraints, schedule and any other factors that assist with the

execution of the penetration. At a minimum, the scope of the Plan **SHOULD** include both Black Box and White Box system testing.

- Document the tests conducted and their results in a Penetration Testing Report.
- Implement remediation activities to rectify issues identified by the security tests.

Retain all testing records for a period of no less than two years after the tests have been completed to allow review by the accreditation assessor.

4 References

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

1. Attorney General's Department, 2017, '*Protective Security Policy Framework (PSPF)',* Australian Government, Canberra. https://www.protectivesecurity.gov.au/Pages/default.aspx
2. Australian Signals Directorate, 2017, '*2017 Australian Government Information Security Manual: Controls (ISM)',* Australian Government, Canberra. https://www.asd.gov.au/infosec/ism/

Annex A: Compliance ratings

Refer to the *TDIF: Risk Management Requirements* for a description of likelihood and consequence ratings.

The following table lists the compliance ratings to be used when undertaking an IRAP Assessment.

Table 1: compliance ratings

COMPLIANCE RATING	DEFINITION
PASS	An IRAP Assessor's determination that the Applicant complies with the protective security requirements of the Trust Framework **MUST** be classified as a pass.
FAIL: CRITICAL	An IRAP Assessor's determination that the Applicant does not comply with protective security requirements of the Trust Framework that may result in Extreme unmitigated risk **MUST** be classified as a critical failure. For example, the inappropriate storage of cryptographic keys, digital certificates or passphrases will be classified as a critical non-compliance. Critical failures **MUST** result in a failed evaluation. The cessation of Trust Framework accreditation activities **MUST** occur until the critical non-compliance is addressed.
FAIL: MAJOR	An IRAP Assessor's determination that the Applicant does not comply with protective security requirements of the Trust Framework that may result in High unmitigated risk **MUST** be classified as a major non-compliance. For example, the Applicant does not have sufficient security awareness training programmes in place will be classified as a major non-compliance. Escalation to a critical non-compliance **MUST** be imposed if: Additional events simultaneously impact the Applicant's identity service. The Applicant attempts to remediate the major non-compliance once and is unsuccessful. Major Failures **MUST** result in a failed evaluation. The Trust Framework Accreditation Authority **MUST NOT** grant accreditation to the Applicant until all major non-compliances are addressed.
FAIL: PARTIAL	An IRAP Assessor's determination that the Applicant does not comply with protective security requirements of the Trust Framework that may result in Moderate unmitigated risk **MUST** be classified as a partial non-compliance. For example, the Applicant's Standard Operating Procedures are not implemented in a manner consistent with their System Security Plan. Escalation to a major non-compliance **MUST** be imposed if: Additional events simultaneously impact the Applicant's identity service. The Applicant attempts to remediate the partial non-compliance twice and is unsuccessful on both attempts. Partial Failures **SHOULD** result in a failed evaluation. The Trust Framework Accreditation Authority **MAY** grant conditional accreditation to the Applicant and request the partial non-compliance be resolved within a period not exceeding six months from the date of accreditation. Once this period has elapsed the Applicant **MUST** demonstrate to the Accreditation Authority that the partial non-compliance has been addressed.

COMPLIANCE RATING	DEFINITION
FAIL: MINOR	An IRAP Assessor's determination that the Applicant does not comply with protective security requirements of the Trust Framework that may result in Low unmitigated risk **MUST** be classified as a minor noncompliance. For example, inconsistencies between document titles, versions, version history and document footer information. Escalation to a partial non-compliance **MUST** be imposed if: Additional events simultaneously impact the Applicant's identity service. The Applicant attempts to remediate the minor non-compliance thrice and is unsuccessful on all three attempts. Minor Failures **MAY** result in a failed evaluation. The Trust Framework Accreditation Authority **MAY** grant conditional accreditation to the Applicant and request the minor non-compliance be resolved within a period not exceeding twelve months from the date of accreditation. The area concerned **MUST** be reviewed as part of the Applicant's annual compliance audit.
NOT APPLICABLE	An IRAP Assessor's determination that a particular protective security control is not applicable to the Applicant's identity service or the Trust Framework Accreditation Authority has accepted a waiver against a particular control.

Annex B: Compliance reporting template

The table below shows the compliance reporting template.

Table 2: compliance reporting template

Domain: {Protective security domain} | **Domain controls**: {number}		
Compliant controls: *{number}* **Non-compliant controls:** *{number}* **Not Applicable controls**: *{number}*		
IRAP Assessor's comments on non-compliant controls		
IRAP Control Number	Compliance Rating	Recommended actions to address residual risk
{control number}	*{as per Annex A}*	

The table below is an example of a compliance reporting template with information added.

Table 3: example of a completed compliance reporting template

Domain: Acquisition, development and maintenance | **Domain** controls: 35		
Compliant controls: 33 **Non-compliant controls:** 1 **Not Applicable controls**: 1		
IRAP Assessor's comments on non-compliant controls		
IRAP control number	**Compliance Rating**	**Recommended actions to address residual risk**
542	PASS	
543	PASS	
544	PASS	
545	NOT APPLICABLE	
550	FAIL: MINOR	*It's recommended the Applicant does <<remediation action>> within the first year of accreditation and demonstrate <<identified issue>> has been remediated to the Trust Framework Accreditation Authority's satisfaction as part of their annual compliance audit.*