Penetration Test

**Functional Assessment Report  
<Applicant Name>**<Initial Accreditation><Annual Assessment><Date>

**Digital Transformation Agency (DTA)**

This work is copyright. Apart from any use as permitted under the Copyright Act 1968 and the rights explicitly granted below, all rights are reserved.

**Licence**

With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (<http://creativecommons.org/licenses/by/4.0/legalcode>)

This licence lets you distribute, remix, tweak and build upon this work, even commercially, as long as they credit the DTA for the original creation. Except where otherwise noted, any reference to, reuse or distribution of part or all of this work must include the following attribution:

*Trusted Digital Identity Framework (TDIF)™* Commonwealth of Australia (Digital Transformation Agency) 2022

**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 Participants*, 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.

**Template - Contact us**

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

**Template management**

The DTA has endorsed this template for release.

**Template Change log**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Version** | **Release Version** | **Date** | **Author** | **Description of the changes** |
| 1.0 | 4.6 | April 2022 | JK | Development of Template for TDIF Release 4.6 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Contents

[1 Response to Findings (Applicant to Complete) 1](#_Toc100662959)

[2 Details 1](#_Toc100662960)

[2.1 Applicant Details 1](#_Toc100662961)

[2.2 Assessor TDIF Requirements 1](#_Toc100662962)

[2.3 Assessor Details 2](#_Toc100662963)

[3 Functional Assessment Report 3](#_Toc100662964)

[3.1 Penetration Test Criteria (Applicant to complete) 3](#_Toc100662965)

[3.2 Testing (Assessor to complete) 4](#_Toc100662966)

[3.3 Test Results (Assessor to complete) 5](#_Toc100662967)

[4 Penetration Test (Functional Assessment) 1](#_Toc100662968)

# Response to Findings (Applicant to Complete)

Include the summary of findings for the *Penetration Test* and your (the Applicant’s) response to each recommendation, risk or non-compliance identified by the *Assessor*. This response must comply with requirements: ASSESS-07-04-02, ASSESS-07-04-03, ASSESS-07-04-03a and ASSESS-07-04-03b.

The Applicant’s Accountable Executive must sign off on the details and date of all remediation activities.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| TDIF Requirement and text | Assessor Findings | Risk Rating[[1]](#footnote-2) | Assessor Recommendation | Applicant Response including statement of acceptance, details of the actions the Applicant will take for remediation | Date of implementation of mitigations | Expected Residual Risk Rating[[2]](#footnote-3) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Details

## Applicant Details

|  |  |
| --- | --- |
| Applicant Details: |  |
| Address |  |
| Date of assessment: |  |
| Period of assessment: |  |
| Accreditation Date[[3]](#footnote-4): |  |
| Accountable Executive |  |

## Assessor TDIF Requirements

|  |
| --- |
| **TDIF Req:** ASSESS-07-02-01; **Updated:** Mar-22; **Applicability:** A, C, I, X  The Applicant MUST demonstrate to the DTA how the Assessors have relevant, reasonable, and adequate experience, training and qualifications to conduct the relevant Functional Assessment |
| **TDIF Req:** ASSESS-07-02-02; **Updated:** Mar-22; **Applicability:** A, C, I, X  The Applicant MUST demonstrate to the DTA how the Assessors:   * Are independent from the development and operational teams of the Applicant’s Identity System * Do not possess a conflict of interest in performing the Functional Assessment. |

## Assessor Details

|  |  |
| --- | --- |
| Assessor Details |  |
| Name of Assessor: |  |
| Role/Position: |  |
| Contact Details |  |
| Statement of experience, training and qualifications: |  |
| Statement of independence[[4]](#footnote-5) |  |
| Conflict of interest statement[[5]](#footnote-6) |  |

# Functional Assessment Report

**Responsible Officers**

|  |  |
| --- | --- |
| *Penetration Test* Report Drafter | Name:  Email: |
| Project Manager | Name:  Email: |
| Accountable Executive | Name:  Position Email: |
| Accountable Executive sign off acknowledgement of *Penetration Test* | Name: Position: Email: Signature (or equivalent) |

## Penetration Test Criteria (Applicant to complete)

|  |
| --- |
| Provide a summary of activities performed by the Assessor during the *Penetration Test, including elements or features of the system requested to be test and limitation placed on the tester. E.g. Only non-destructive Testing, use of Pre-Production only.* |
|  |

## Testing (Assessor to complete)

|  |
| --- |
| **TDIF Req:** ASSESS-07-01-02; **Updated**: Mar-22; **Applicability**: A, C, I, X  The *Applicant MUST:*   1. define and prepare written instructions on the scope, objectives and criteria for each *Functional Assessment* 2. ensure such written instructions are consistent with the TDIF requirements 3. provide a copy of such instructions to the relevant *Assessor* prior to commencement of the *Functional Assessment*; and 4. ensure that each *Functional Assessment* is conducted in accordance with such written instructions. |

|  |
| --- |
| What was the test or evaluation methodology used, including what features or elements of the Applicant’s system were penetration tested? |
|  |

|  |
| --- |
| List any significant questions from the *Assessor* and responses by the *Applicant*: |
|  |

|  |
| --- |
| Assessor’s documentation review details (if applicable, for example to the scoping or undertaking the penetration test) |
|  |

|  |
| --- |
| List interviews with key *personnel* conducted as part of the *assessment*: (if applicable, for example, to the scoping or undertaking the Penetration test). |
|  |

## Test Results (Assessor to complete)

|  |
| --- |
| Provide an overview of the *Applicant’s Identity System,* for Pen tests this is normally what parts or elements of the system were pen tested: |
|  |

|  |
| --- |
| What are the test or evaluation results? This can include references to artefacts holding the list and details of adverse findings where appropriate. |
|  |

|  |
| --- |
| List any assessment criteria or observation that could not be assessed due to access, timing issues, or other impediments. These can be limitations to the scope of the pen testing. |
|  |

# Penetration Test (Functional Assessment)

|  |
| --- |
| **TDIF Req:** ASSESS-07-06-02; **Updated**: Mar-22; **Applicability**: A, C, I, X  The *Applicant MUST* commission an *Assessor* to conduct a *Penetration Test* of:   1. its *Identity System*; and 2. each major production release of software forming part of its *Identity System* following accreditation. |

A *Penetration Test* is a sensitive security assessment. An *Applicant* should be aware of the security risks involved in sharing this information. Therefore the DTA may review the *Penetration Test* results over a secure video call or via a visit to the *Applicant’s* site of operations or office.

1. As per Appendix A: Risk Ratings of TDIF 04 Functional Requirements (for initial assessments) or TDIF 07 Maintain Accreditation (for the Annual Assessment) . The Applicant must provide a copy of their own risk framework to the DTA for assessment. [↑](#footnote-ref-2)
2. Once the recommendation or fix is implemented [↑](#footnote-ref-3)
3. If this is an assessment for initial accreditation, please insert the expected accreditation date. [↑](#footnote-ref-4)
4. Demonstrate how the assessor is independent from the development and operational teams of the *Applicant’s TDIF Accredited System.* [↑](#footnote-ref-5)
5. The Applicant MUST demonstrate to the DTA how the Assessor does not possess a conflict of interest in performing the Functional Assessment. [↑](#footnote-ref-6)