A black and green background

AI-generated content may be incorrect.

Independent privacy evaluation for [Provider name] and [Service name]

[Date]

DRAFT V2.0 July 2025

# Contents

[Contents 1](#_Toc202365483)

[About this guidance 3](#_Toc202365484)

[Structure of the evaluation 4](#_Toc202365485)

[Introduction 5](#_Toc202365486)

[Evaluation details 5](#_Toc202365487)

[Approach 6](#_Toc202365488)

[About this template 6](#_Toc202365489)

[Completing a privacy evaluation 8](#_Toc202365490)

[Introduction 8](#_Toc202365491)

[Components of the privacy evaluation 9](#_Toc202365492)

[Privacy evaluation 10](#_Toc202365493)

[Findings and remediations 14](#_Toc202365494)

[Information and additional evidence used to inform your evaluation 15](#_Toc202365495)

[Appendix A - Glossary 16](#_Toc202365496)

# About this guidance

As regulator, the Trust Framework Authority assesses and accredits providers, and their services, against the Trust Framework legislation.

Independent privacy evaluators play a role in the evaluation of providers seeking accreditation under the Digital Identity Services Trust Framework (the Trust Framework).

Independent privacy evaluators provide an evaluation on whether the provider meets the requirements of the Trust Framework Authority as set out in [legislation](https://www.dia.govt.nz/Trust-Framework-for-Digital-Identity-Legislation#:~:text=The%20Trust%20Framework%20Rules%20establish%20the%20technical%20and,on%20the%20recommendation%20of%20the%20Trust%20Framework%20Board.) including the Digital Identity Services Trust Framework Act (the Act), the Privacy Act 2020, the Digital Identity Services Trust Framework Regulations 2024 (the regulations) and the Service standards and processes set out in the Digital Identity Services Trust Framework Rules 2024. (the Trust Framework Rules).

The Trust Framework Authority will make the final assessment and accreditation decision.

If you have questions about the evaluation process or this guidance, or need assistance, please contact [TFA@dia.govt.nz](mailto:TFA@dia.govt.nz).

# Structure of the evaluation

This template is for use by independent privacy evaluators.

Sections in blue may be deleted after the evaluation is completed.

The provider will:

* Select an independent evaluator to use from the list of evaluators considered by the Trust Framework Authority to have the appropriate skills, knowledge and experience to conduct privacy evaluations. One independent privacy evaluator should perform all aspects of the evaluation including reviewing and assessing all documentation provided, even if the independent evaluator has also conducted the Privacy Impact Assessment.
* Agree pricing with the independent evaluator.
* Provide the independent evaluator with the information and documentation, and where appropriate access to systems and processes, to enable the evaluator to carry out the independent evaluation.
* Respond to any questions or requests for additional information from the independent evaluator.
* Submit the completed evaluation, documentation and all materials used to complete the evaluation to the Trust Framework Authority for assessment.

The independent evaluator will:

* Agree pricing with the provider.
* Receive a documents and information from the provider.
* Ask the provider for the additional information needed to complete the evaluation.
* Complete the evaluation using the information provided, along with a combination of interviews, walkthroughs, observations, and detailed testing if needed.

**Inputs to the evaluation**

When completing your evaluation please save copies of all documentation that you use. This should include:

* Any additional documents that you request from the provider.
* Any screen shots you take of the provider’s system(s).
* Notes you make of discussions or interviews with representatives from the provider.

These must be listed in the section on information and additional evidence used to inform your evaluation. They need to be given to the provider for them to submit to the Trust Framework Authority as part of their application for accreditation.

# Introduction

This document records the privacy evaluation for [Provider Name] for [Service Name].

## Evaluation details

| Evaluation details | |
| --- | --- |
| Provider |  |
| Date submitted |  |
| Service name |  |
| Digital identity services applied for |  |
| Evaluator |  |
| Evaluator organisation |  |
| Reviewer (if relevant) |  |
| Date evaluation completed |  |
| Template version | V2.0 |

# Approach

## About this template

This template was developed to support the evaluation of providers who intend to apply for Trust Framework accreditation. It is a tool for independent privacy evaluators to record their evaluation findings. It can also be used by providers to prepare evidence of controls for their evaluation.

Text in blue is instructions for the independent evaluator and can be removed from the final version of the evaluation.

Purpose

This document provides an independent privacy evaluation of [Service Name] for [Provider Name]. The following methodology was used to complete the evaluation:



It involved the following steps:

1. **Conducting a privacy impact assessment** – Conducting a Privacy Impact Assessment, completed by either the provider or the independent evaluators.
2. **Completing a privacy evaluation** Evaluation of the compliance with privacy expectations and requirements relevant to the digital identity service.
3. **Confirming conclusions and remediations** - Confirmation of the conclusions and their planned or actioned remediations that have been identified in the evaluation of the controls and risks.
4. **Documenting information used and additional evidence -** Documentation of information used to inform the evaluation including documents, interviews, and additional evidence such as screen shots or notes from discussions.

Completing a privacy evaluation



## Introduction

The privacy expectations and requirements detailed in this template align directly to those detailed in the Trust Framework Rules and relevant parts of the Privacy Act 2020. The last three expectations listed are captured by the expectation to comply with the Information Privacy Principles within the Privacy Act. While these should also be addressed through the review of the Privacy Impact Assessment, due to the importance of these in the context of digital identity services, they have also been included separately.

Providers need to have the opportunity to respond to the evaluation, particularly where the evaluator concludes that the privacy environment or parts of it are not appropriate. This may include providing context on the issue, whether there are compensating controls in place, or existing plans to remediate the issue and the timeframes for this to occur.

Where the conclusion is that arrangements or controls are not sufficient, the provider may want to make the changes recommended by the independent evaluator in the findings section of this document and resubmit to the independent evaluator for re-evaluation.

## Components of the privacy evaluation

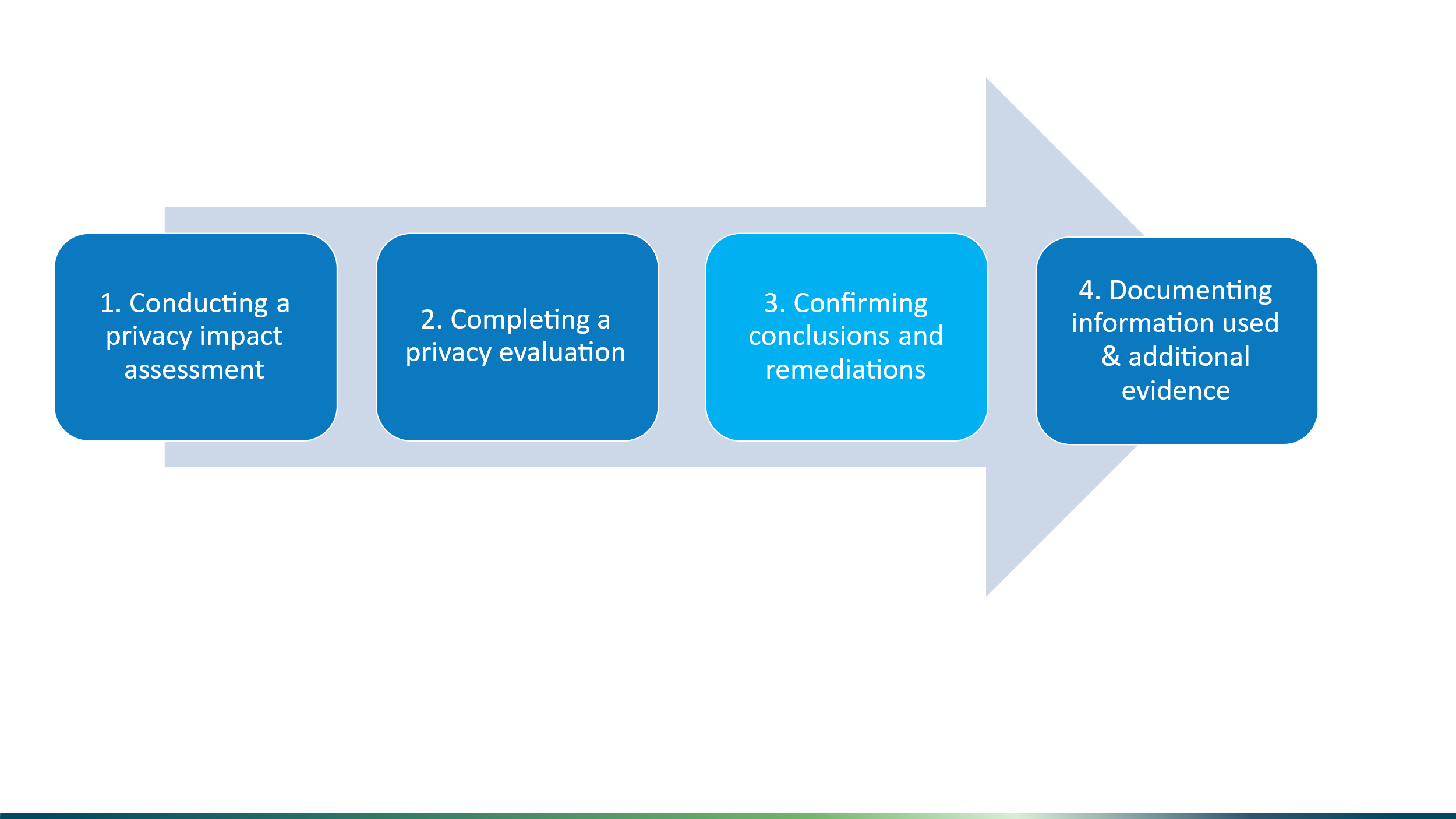
**Table 1 – Control validation components**

| **Component** | **Description** |
| --- | --- |
| ID | The identification number for each privacy expectation/requirement. |
| Expectation/requirement | Privacy-related requirements and expectations for the delivery of accredited digital identity services. |
| Referenced standards | The relevant aspect of the Privacy Act 2020 and Trust Framework Rules. |
| Evaluation methodology | How the independent evaluator should evaluate whether the expectations and requirements are being met. |
| Evidence gathered | The evidence gathered by the independent evaluator in this evaluation. Formal evaluation may take place using interviews, walkthroughs, observations and a review of technical evidence. Where needed, detailed testing is conducted.  Relevant screenshots and additional evidence provided should be included in the section **Information and additional evidence used to inform your evaluation**.  The use of any independent evaluation reports should also be listed here, such as internal audit reports about privacy. |
| Conclusions | Overall conclusion of whether the provider and service appropriately meet the expectations and requirements of good privacy management. This may include any outstanding (unaddressed) recommendations. |

# Privacy evaluation

| ID | Expectation/Requirement | Referenced standards or Trust Framework Rules | Evaluation methodology | Evaluation | Evidence gathered | Conclusions |
| --- | --- | --- | --- | --- | --- | --- |
| **C01** | **Privacy Impact Assessment**   * A Privacy Impact Assessment has been completed for the service. * The Privacy Impact Assessment is reviewed at least every two years or following any significant change to the service. | **Rules**  12(2)  12(3)  12(4) | * Confirm that a Privacy Impact Assessment (PIA) has been completed for the accredited service and that it assesses (as a minimum):   + The detailed services being provided.   + What information is already held and new information to be collected.   + The specific purpose/s for which the personal information is collected and/or used.   + The information flows between people, systems and processes within the organisation (either in diagram or text format).   + How information will be stored, accessed, used and disposed of.   + The privacy risks that the service creates or may create.   + What controls are in place to mitigate those risks. * Confirm that the PIA has been formally approved by the Provider. * Confirm that a mechanism is in place to ensure that the PIA is updated every two years, or following any significant change that has occurred to the services offered. * Verify that any identified risks outlined in the PIA have been appropriately addressed. * Where a relevant Code of Practice exists, confirm that the Code of Practice is sufficiently considered within the PIA. |  |  |  |
| **C02** | **Designated individual**   * A designated individual who is responsible for privacy is appointed (note that this may be the Privacy Officer per the Privacy Act 2020). | **Rules**  12(5) | * Confirm that a designated individual has been appointed. * Where appropriate, validate that the designated individual’s responsibilities are detailed in their position description and include:   + Overseeing the PIA process and review of the PIA.   + Ensuring compliance with all applicable laws, regulations, and codes.   + Managing privacy policies.   + Monitoring privacy risks and compliance. |  |  |  |
| **C03** | **Privacy training**   * Staff are provided regular privacy awareness training. * Staff are made aware of any changes to privacy policies and processes. | **Rules**  12(6)  12(7) | * Confirm that the provider’s privacy policy is readily available to staff (e.g. through publishing on the intranet). * Confirm that privacy awareness training takes place when all relevant staff (including contractors) initially join the provider, and then on an ongoing basis. * Confirm that the privacy awareness training includes details on:   + Lawful purposes and uses for personal and organisational information collected and held by the provider.   + Processes to amend or update a user’s personal or organisational information when requested by that person.   + Processes regarding storage, use and disclosure of information.   + Awareness of privacy complaints and incidents procedures.   + How to identify and escalate a potential privacy breach. * Confirm that a structured process is in place to follow-up on any staff who have not completed the privacy awareness training in the timeframes expected. * Verify for a sample of new starters during the past year that they have completed their privacy training as expected through inspecting the training records. * Confirm that a formal process is in place to make staff aware of any changes to the provider’s privacy policies and processes. * Determine if there have been any changes made to the provider’s privacy policies and processes (or should have been because of changes having been made to the Privacy Act) and verify that staff were made aware of the changes and the impact of those changes. |  |  |  |
| **C04** | **Privacy Incident Management**   * A Privacy Incident Response Plan is in place defining how the provider responds to privacy incidents. * A privacy incident register is maintained. * A formal data breach reporting process is established. | **Rules**  12(8)  12(9)  12(10)  **Privacy Act**  s113  s114  s115 | * Confirm that a formal Privacy Incident Response Plan is established and that it:   + Clearly defines the roles and responsibilities for managing a suspected privacy incident.   + Addresses all forms of incidents, including notifiable breaches and less significant breaches or near misses.   + Includes the processes for:     - Escalation and notification.     - Containing and assessing an incident.   + Outlines the timeframe for when to report a notifiable breach, and for reporting a notifiable breach to the Office of the Privacy Commissioner and affected users (and that those timeframes comply with Office of the Privacy expectations of reporting a breach to them within 72 hours of becoming aware of the breach).   + Requires any privacy breaches related to an accredited service to be reported to the Trust Framework Authority as soon as the provider is practically able to do so. * Confirm that a privacy incident register is maintained to record and track all privacy incidents (both actual and near misses), and that the register contains sufficient information such as:   + Time, date, and country of origin.   + Description of the circumstances.   + Whether the incident was deliberate or accidental.   + An assessment of the size and impact of the incident.   + A summary of actions taken to resolve the incident. * Review the privacy incident register and identify any significant incidents over the past 12 months. Confirm that:   + They have been reported to Office of the Privacy Commissioner and affected users (where a notifiable breach has occurred).   + The provider’s processes and controls have been modified (where relevant) to minimise the likelihood of a similar incident occurring in the future. |  |  |  |
| **C05** | **Privacy Statement**   * A Privacy Statement, or appropriate alternative, is in place. | **Rules**  12(11)  **Privacy Act**  IPP 3 | * Confirm that a Privacy Statement or appropriate alternative exists, and that the information outlined within it is consistent with Information Privacy Principle 3 of the Privacy Act 2020, including details about:   + That personal information is being collected (if it’s not obvious).   + Why the information is being collected.   + What the information is going to be used for.   + Who the information will be given to (if anyone), including any third party providers.   + Whether the information must be given, and what will happen if it is not provided.   + How the information can be accessed, and how it can be corrected if it is wrong. * Verify that the Privacy Statement or appropriate alternative is readily made available to users. * Confirm that the Privacy Statement has been reviewed in the past 12 months. |  |  |  |
| **C06** | **Secondary use**   * Personal information must not be used for secondary purposes unless explicitly authorised. | **Rules**  12(12)  **Privacy Act**  IPP 10 | * Confirm that either:   + The secondary use of personal information is explicitly prohibited; or   + A formal process is in place to manage requests to use personal information for secondary purposes, and that the process requires the explicit authorisation of the user prior to any secondary use. * Where personal information is used for a secondary purpose, verify for a sample of users that explicit authorisation by the user has been received. |  |  |  |
| **C07** | **Privacy-related requests, complaints and concerns (if required)**   * Users have access to a mechanism to communicate privacy related requests, complaints and concerns. | **Privacy Act**  IPP 6  IPP 7 | * Confirm that formal processes are established to manage privacy related requests, complaints and concerns, including:   + Requests to confirm what personnel information is held by the provider.   + Requests to correct personal information.   + Complaints related to privacy. |  |  |  |
| **C08** | **Data minimisation**   * Only the minimum amount of personal information necessary is collected. * A retention period is established, and personal information is disposed of when there is no longer a need to retain it. | **Privacy Act** IPP 1  IPP 9 | * Determine what personal information is collected for the service and confirm that a justifiable business need has been established for each type of information. * Confirm that a formal data retention policy is in place, and that the policy:   + Defines the retention period for the personal information retained.   + Details the business purpose for keeping the information for the specific period. * Confirm that a formal data disposal process is in place to dispose of personal information when it is no longer needed, and that a process is in place to identify data that has reached the retention period and should be disposed of. |  |  |  |
| **C09** | **International transfers (if required)**   * Personal information is only made available to overseas organisations where there are comparable safeguards to New Zealand. | **Privacy Act**  IPP 12 | * Identify what overseas organisations personal information is disclosed to and verify that an analysis has been performed to confirm that:   + The overseas organisation is subject to the Privacy Act because they do business in New Zealand; or   + Contractual clauses have been used to ensure the information will be adequately protected; or   + The overseas organisation is subject to privacy laws that provide comparable safeguards to the Privacy Act. |  |  |  |

# Findings and remediations



Only findings that require remediation should be listed here. If a finding is marked as requiring remediation by the independent evaluator, it must be addressed before submitting the evaluation to the Trust Framework Authority. The following table summarises the findings (deficiencies) that have been identified during the evaluation:

| **Conclusion ID** | **Conclusion** | **Expectation/ Requirement** | **Planned remediation** | **Planned remediation date** | **Status** |
| --- | --- | --- | --- | --- | --- |
| F01 |  |  |  |  | Open/ Resolved/ In-Progress/ Compensating Controls Applied |
| F02 |  |  |  |  |  |
| F03 |  |  |  |  |  |
| F04 |  |  |  |  |  |

# Information and additional evidence used to inform your evaluation



The following documents were reviewed to inform this privacy evaluation:

| **Document name** | **Version** | **Date** |
| --- | --- | --- |
|  |  |  |

The following interviews and workshops were held to inform this privacy evaluation:

| **Interviewee/s** | **Date** |
| --- | --- |
|  |  |

The following evidence was provided to support the evaluation, which is relevant to this evaluation:

You may include here any of the following that are not recorded in separate documents:

* Any screen shots you take of the provider systems.
* Notes you make of discussions or interviews with representatives from the provider.

Appendix A - Glossary

| **Term** | **Definition** |
| --- | --- |
| Personal Information | Person information has the meaning as in section 7(1) of the Privacy Act 2020. personal or organisational information means – (a) information that describes the identity of an individual or organisation: (b) other information about that individual or organisation. |
| Privacy Act | [Privacy Act 2020](http://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html). This governs how organisations in New Zealand should collect, handle, and use personal information. |
| Privacy Codes of Practice | The [Privacy Codes of Practice](https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/) outline Privacy Rules for personal information in specific areas, such as health, telecommunications, and credit reporting. |
| Privacy Impact Assessment | A Privacy Impact Assessment (PIA) is a way for organisations to assess and address privacy risks when they are collecting, using, or sharing personal information. A PIA helps:   1. Check whether a service complies with privacy laws. 2. Identify and minimise privacy risks (e.g. data breaches). 3. Give users certainty that their information is safe. 4. Improve information management systems. |
| Trust Framework Provider | An accredited provider of any digital identity service. Usually referred to as a Trust Framework Provider. The definition is defined in section 5 of the Digital Identity Services Trust Framework Act 2023. |
| User | An individual who:   1. shares personal or organisational information, in a transaction with a relying party, through one or more accredited digital identity services; and. 2. does so for themselves or on behalf of another individual or an organisation. |