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

[Date]

v1.2 July 2025

# Contents

[About this guidance 3](#_Toc202374387)

[Structure of the evaluation 4](#_Toc202374388)

[Introduction 5](#_Toc202374389)

[Evaluation details 5](#_Toc202374390)

[Approach 6](#_Toc202374391)

[About this template 6](#_Toc202374392)

[Controls validation guidance 8](#_Toc202374393)

[Introduction 8](#_Toc202374394)

[Components of the control evaluation 9](#_Toc202374395)

[Control validation 11](#_Toc202374396)

[Risk evaluation guidelines 31](#_Toc202374397)

[Introduction 31](#_Toc202374398)

[Components of the risk evaluation 32](#_Toc202374399)

[Risk evaluation 36](#_Toc202374400)

[Security risk position 42](#_Toc202374401)

[Findings and remediations 43](#_Toc202374402)

[Information and additional evidence used to inform your evaluation 44](#_Toc202374403)

[Appendix A - Risks applicable for each Digital Identity Service 45](#_Toc202374404)

[Appendix B - Glossary 46](#_Toc202374405)

# About this guidance

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

Independent security evaluators play a role in the evaluation of providers seeking accreditation under the Digital Identity Services Trust Framework (the Trust Framework). Independent security evaluators provide an evaluation on whether the provider meets the requirements of the Trust Framework Authority as set out in legislation including the Digital Identity Services Trust Framework Act (the Act), the Privacy Act 202, and 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 the Trust Framework Authority at [TFA@dia.govt.nz](mailto:TFA@dia.govt.nz).

# Structure of the evaluation

This template is for use by independent security evaluators. Text in blue provides guidance for completing the evaluation and can be removed from the final version.

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 security evaluations. One independent security evaluator should perform all aspects of the evaluation including reviewing and assessing all documentation provided.
* Agree pricing with the independent evaluator.
* Send the completed **Trust Framework Authority scope for independent security evaluation template** and relevant information and documentation to the independent evaluator.
* Respond to any questions or requests for additional information from the independent evaluator.
* Submit the completed evaluation and all materials used to complete the evaluation to the Trust Framework Authority for assessment, with the remainder of the application.

The independent evaluator will:

* Agree pricing with the provider.
* Receive a completed **Trust Framework Authority independent security evaluation template** and relevant information and documentation from the provider.
* Ask the provider for any additional information needed to complete the evaluation.
* Complete the evaluation using the information provided, along with a combination of interviews, walkthroughs, observations, review of technical documentation, and detailed testing if needed.

**Inputs to the evaluation**

When completing your evaluation, please save copies of all documentation 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 used to inform your evaluation. Documents must be given to the provider for them to submit to the Trust Framework Authority as part of their accreditation application.

# Introduction

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

## Evaluation details

| Evaluation details | |
| --- | --- |
| Provider |  |
| Date submitted |  |
| Service name(s) |  |
| Digital identity services applied for |  |
| Evaluator |  |
| Evaluator organisation |  |
| Reviewer (if relevant) |  |
| Date evaluation completed |  |
| Template version | v1.2 |

# 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 security evaluators to record their evaluation findings. It can also be used by providers to prepare evidence of controls for their evaluation.

This document is one of two documents to support the security evaluation. The document is shown in context in the diagram below.

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 security risk evaluation of [Service Name] for [Provider Name]. The following methodology was used to complete the evaluation:



It involves the following steps:

1. **Completing a controls validation**– Evaluation of the effectiveness of each control relevant for the digital identity service. This is done through:

* Interviews.
* Walkthroughs.
* Observations.
* A review of technical evidence.
* Detailed testing if needed.

1. **Conducting a risk evaluation** - Evaluation of the relevant risks for the digital identity service. This is determined through analysing the likelihood and impact of the risk occurring given the mitigation provided by the controls.
2. **Identifying the security risk position** – Mapping each assessed risk to provide an overall security risk position for the digital identity service.
3. **Confirming findings and remediations** - Confirmation of the findings and their planned or actioned remediations that have been identified in the evaluation of the controls and risks.
4. **Documenting the 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.

Controls validation guidance

1. Completing a controls validation

2.Conducting a risk evaluation

3. Identifying the security risk position

4. Confirming findings and remediations

5. Documenting information used and additional evidence

## Introduction

The controls validation involves evaluating the effectiveness of each of the 20 recommended security controls. This is done by the independent evaluator:

* Reviewing any independent evaluation reports that have been agreed as part of the scope.
* Reviewing technical evidence such as independent technical testing.
* Gathering information through interviews, walkthroughs and observations.
* Reviewing system outputs.
* Testing if needed.

Providers need to have the opportunity to respond to the control evaluation, particularly where the control is assessed as partially effective or not effective. 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.

The controls evaluation informs the risk evaluation, which identifies the extent to which the controls mitigate the risks.

Where controls are evaluated as partially effective or not effective, 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. This may be driven by the risk evaluation, and by which controls are needed to meet the acceptable risk level.

## Components of the control evaluation

**Table 1 – Control validation components**

| **Component** | **Description** |
| --- | --- |
| Control ID | The identification number for the control. |
| Control title and objectives | The name of the control, and what the control aims to achieve. |
| Associated risks  (Gross score) | The risks that the control is designed to mitigate, and the risk rating for the risk with no controls in place. |
| Referenced standards | Standards that may be used to contribute to the evaluation of the control. |
| Evaluation methodology | How the independent evaluator will evaluate the effectiveness of the control. |
| Evaluation | What the independent evaluator did to determine the effectiveness of the control and what conclusions they reached based on their findings. This should include:   * Whether the controls have been implemented and correctly configured. * Whether they are working as intended. * How they have been tested. * Whether they are effective.   The evaluation should include any responses provided by the provider in response to the evaluation, such as:   * Whether there are compensating controls in place to address the issue. * If there are already plans in place to remediate the issue and when this will occur. * Any other details to provide context on the issue. |
| Evidence gathered | The evidence gathered by the independent evaluator to evaluate this control. Formal evaluation takes place using interviews, walkthroughs, observations and a review of technical evidence. Where needed, detailed testing is conducted. Relevant screenshots and additional evidence provided to highlight the effectiveness of controls 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:   * ISAE 3402 / SOC 2 reports. * Reports on compliance with NZISM v3.8[[1]](#footnote-2). * ISO27001 certification and Statement of Applicability[[2]](#footnote-3). |
| Control effectiveness | The effectiveness of the control using the guidance in **Table 2**. |

Effectiveness evaluation

**Table 2 – Control effectiveness descriptions**

| **Effectiveness** | **Description** |
| --- | --- |
| **Effective** | The control has been implemented and is operating as designed. |
| **Partially effective** | Minor deficiencies have been highlighted with the implementation of the control, or the control has not been in place long enough to determine its effectiveness. |
| **Not effective** | Major deficiencies have been highlighted with the implementation of the control, or the control has not been implemented. |
| **Not assessed** | The control could not be assessed. |

# Control validation

| Control ID | Control title and objectives | Associated risks  (Gross score) | Referenced standards or Trust Framework Rules | Recommended evaluation methodology | Evaluation | Evidence gathered | Control effectiveness |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **C01** | **User access management**   * A role-based access control model is used to manage access to the system(s). * The access that each role should be granted is formally defined and users are only provided the minimum access they require to perform their roles. * A formal user access management process is in place and consistently followed to manage the:   + Granting of access to systems, including granting privileged access to systems.   + Changing of access to systems (e.g., when someone changes roles).   + Review of access to systems.   + Revocation of access to systems. * A user’s access is revoked in a timely manner when they leave an organisation. * Users’ access to systems is formally reviewed on a periodic basis. * Shared user accounts are not used unless necessary, and then only if the identity of a person using a shared account can be positively confirmed through another mechanism. | DIS.R01 (High)  DIS.R05 (Critical)  DIS.R09 (High)  DIS.R11 (High) | **NZISM**  16.2  **ISO27002**  5.3  5.37  5.15  5.16  5.18  **Rules**  13(1) – 13(5)  16(3) – 16(4) | * Verify that the access rights that each role should hold within a system are documented e.g., within a RBAC (Role-Based Access Control) matrix. * Verify that formal procedures are established to grant, change, review, and revoke user access to the systems. * Confirm that the RBAC matrixes (or similar) established are used as a basis to grant, modify, and review access. * Confirm that any user access outside of that established in the RBAC matrixes (or similar) requires approval of the system owner before being granted. * Verify that user access reviews are performed on at least a six-monthly basis, and that:   + The reviews are documented.   + The reviews consider whether:     - Users continue to work for the organisation, and     - Users should continue to have privileged access.   + The results of the reviews are approved by each system owner. * Verify that user access reviews have been recently performed for a sample of systems (including any central identity mechanisms used to authenticate staff). * Confirm that the processes to revoke access ensure that:   + All user access is removed on or before a person’s last day.   + All assets (e.g. computers, smartphones) are returned and accounted for. * Verify for a sample of systems (including any central identity mechanisms used to authenticate staff) that there are no accounts for staff who have left the organisation. * Verify for a sample of systems (including any central identify mechanisms used to authenticate staff) that there are no shared user accounts implemented, and if there is, that:   + A documented business case exists for the use of a shared account.   + The use of a shared account has been formally approved by the system owner.   + The identity of any person using a shared account can be positively confirmed through another mechanism. |  |  |  |
| **C02** | **Authentication**   * Users are required to have robust passwords. * Passwords should be changed on a periodic basis. * Common passwords are not used when user accounts are initially created or when a password is reset. * Accounts should lock indefinitely (i.e., until investigated and reset by an administrator) after repeated failed login attempts. * All authentication to a system (successful or failed) is logged. * Passwords are communicated to users in a secure manner when their account is initially created, or their password is reset. * The identity of a user is positively confirmed when they request their password to be reset. * Documented administrative passwords are stored in a secure manner (such as in a password manager with strong controls). * All passwords are stored in an encrypted manner. * Multi-factor authentication is used by all users for remotely accessing the systems. | DIS.R01 (High)  DIS.R05 (Critical)  DIS.R09 (High)  DIS.R11 (High) | **NZISM**  16.1  16.2  16.7  **ISO27002**  5.17  8.5  **Rules**  13(1) – 13(5) | * Confirm that the organisation’s password standard or policy requires at least the following controls to be implemented:   + Password construction controls that:     - Require a minimum password length of 16 characters with no complexity requirements; or     - Require a minimum password length of ten characters, consisting of at least three of the following character sets:       * Lowercase characters (a-z).       * Uppercase characters (A-Z).       * Digits (0-9).       * Punctuation and special characters.     - Require a password to be different to the last 8 passwords used.     - Prevent sequential passwords from being used e.g., Password123, Password124, Password125.   + Accounts to be locked out:     - After three failed logon attempts within a day.     - Until investigated and reset by an administrator.   + Passwords to be changed every 90 days.   + Passwords to have a minimum age of 1 day before being able to be changed.   + All authentication attempts (successful or unsuccessful) to be logged. * Verify that the above requirements are enforced for a sample of systems (including any central identity mechanisms used to authenticate staff). * Confirm that the passwords for any break-glass accounts or shared administrative accounts are stored in a password manager, and that:   + The password manager limits access to specific groups of passwords based on business need.   + Strong authentication controls are implemented (in line with that outlined above).   + Multi-factor authentication must be used to access the password manager.   + The passwords are stored in an encrypted manner. * Confirm that when accounts are initially created:   + A common or easily guessed password is not issued (where the end user does not choose their own initial password).   + The passwords are securely communicated to the end users and that the users are required to change their initial password the first time they log in (where the end user does not choose their own initial password). * Confirm that the password reset process:   + Positively confirms the identity of a person requesting a password or multi-factor authentication to be reset.   + Has a structured process to handle any exceptions i.e., to handle a situation where a person cannot confirm their identify through the normal mechanisms.   + Does not reset the password to a common or easily guessed password (where the end user does not choose their own new password). * Verify that multi-factor authentication is used for all users for remotely accessing the systems from:   + The Internet.   + Any lower security domain e.g., the corporate network. |  |  |  |
| **C03** | **Privileged access management**   * Privileged user accounts are defined and formally approved. * Privileged user access is tightly controlled. * Multi-factor authentication is used for privileged access. * The ongoing appropriateness of the privileged access granted is reviewed. * The activities of privileged users are logged. * Users are aware of their responsibilities when using privileged accounts. | DIS.R09 (High) | **NZISM**  16.3  16.4  **ISO27002**  8.2  **Rules**  13(1) – 13(5)  16(4) | * Verify that the organisation’s privileged access management standard or policy requires that:   + All privileged user accounts are required to be documented (e.g., in a register) and formally approved by each system owner.   + Multi-factor authentication is used for all privileged accounts (through, for example, the use of a privileged access management system).   + Privileged access reviews are to be performed on at least a six-monthly basis, and that:     - The reviews are documented.     - The reviews to consider both whether:       * Users continue to work for the organisation.       * Users should continue to have privileged access.     - The results of the reviews to be approved by each system owner. * Verify the above requirements are met for a sample of systems (including any central identity mechanisms used to authenticate staff). * Verify that the privileged access management standard or policy includes a response and remediation policy and procedure. * Confirm that continuous monitoring is implemented over privileged accounts, with the following being logged:   + Individual user activity, including exceptions such as out of hours access.   + Activity from unauthorised sources.   + Any unusual use patterns.   + Any creation of unauthorised privileges access credentials. * Confirm that the continuous monitoring logs is protected against alternation. * Confirm that privileged access training is provided to all privileged users as part of the organisation’s training and awareness processes. |  |  |  |
| **C04** | **Encryption**   * All sensitive information sent over networks (including the Internet) is encrypted. * All sensitive information stored within systems is encrypted. * Robust encryption protocols and algorithms are used. * Encryption keys are managed in a structured manner throughout the lifecycle. | DIS.R05 (Critical)  DIS.R10 (High)  DIS.R11 (High) | **NZISM**  17.1  17.2  17.3  17.0  **ISO27002**  8.24  **Rules**  13(1) – 13(5)  14(8) – 14(10) | * Verify that an encryption standard or policy has been documented, and that the standard or policy details:   + What the organisation’s approved cryptographic algorithms are.   + What the organisation’s approved cryptographic protocols are.   + When Key Management Plans are required, and what should be contained within a Key Management Plan.   + What the established cryptoperiods are for all keys and cryptographic implementations. * Verify that approved cryptographic algorithm and protocols meet the requirements of NZISM. * Confirm that all sensitive information is stored in an encrypted manner. * Confirm that all data sent over networks (including the Internet) is encrypted in transit. * Verify through the review of the most recent vulnerability scanning and penetration testing reports that:   + No weak encryption algorithms or protocols were in use.   + No instances of unencrypted traffic were identified. * Verify that a Key Management Plan has been documented for any critical cryptographic systems or processes used to manage the delivery of the services. * Verify that any Key Management Plan documents (at a minimum):   + The objectives of the cryptographic system and Key Management Plan.   + A description of the system.   + Roles and administrative responsibilities.   + Accounting processes.   + How information security incidents will be handled.   + Key management processes.   + Maintenance processes.   + Reference to related vendor documentation and related policies. |  |  |  |
| **C05** | **Secure systems development**   * Development is not done directly in production. * Developers do not have access to production environments. * Code is developed in a secure manner. * Code is reviewed and tested for vulnerabilities before being published. | DIS.R03 (High)  DIS.R05 (High) | **NZISM**  14.4  **ISO27002**  8.25  8.26  8.27  8.28  8.29  8.31  **Rules**  13(1) – 13(5) | * Confirm that development is not done directly in production, and that at least the following three environments exist for all key systems:   + Development.   + Testing.   + Production. * Confirm that the change management process is followed to move code or between development, testing and production. * Verify for a sample of systems that developers do not have access to production. * Verify that secure coding guidelines have been developed and published. * Verify that developers are provided training on secure coding (in addition to the guidelines). * Review the documented SDLC (Systems Development Life Cycle) process and verify that:   + Code is required to be tested for vulnerabilities before being placed into production.   + Code is required to be reviewed by someone other than the developer. * Review the reports from the most recent vulnerability scanning and penetration testing and verify that there were no issues identified that relate to insecure coding practices. |  |  |  |
| **C06** | **Change management**   * All changes to a system are documented and approved through a formal change control process before being implemented. * Any proposed changes are evaluated in terms of their anticipated impact on a system. Roll-back plans are established for any change that has the potential of impacting the security (confidentiality, integrity, or availability) of a system. * An emergency change management process is established to deal with urgent changes. * The segregation of duties implemented prevents one person from both developing and implementing a change in production. * All changes are tested before being placed into production. | DIS.R03 (High)  DIS.R04 (Moderate)  DIS.R06 (Moderate)  DIS.R07 (Critical)  DIS.R10 (High) | **NZISM**  6.3  **ISO27002**  5.37  8.32  8.33  **Rules**  13(1) – 13(5) | * Confirm that a formal change management procedure is established and that it:   + Includes processes to:     - Document changes from request through to implementation.     - Assess and prioritise changes.     - Test changes.     - Establish roll-back plans for any change that has the potential to impact the security of a system.     - Approve changes before they are place into production.     - Handle emergency changes that cannot go through the normal process due to urgency.   + Is used for all changes. * Validate for a sample of changes made to a sample of systems over the past six months, that the changes followed the established change management process. * Confirm that segregation of duties (or sufficient mitigating controls) is in place to prevent someone:   + Both developing and implementing a change.   + Making an unauthorised change to a system i.e., putting a non-approved change through. * Confirm that changes are tested in a non-production environment that replicates the production environment. * Confirm that non-production data is used in non-production environments for testing. |  |  |  |
| **C07** | **Host protection**   * Standard operating environments are established for each technology used to deliver the services. * The standard operating environments are hardened based on best practice standards and/or vendor guidelines. * Up-to-date anti-malware protection is implemented to reduce the likelihood of malicious software being introduced. | DIS.R07 (Critical) | **NZISM**  14.1  **ISO27002**  8.7  **Rules**  13(1) – 13(5) | * Verify that the organisation has standard operating environments established for each key technology utilised. * Verify that the standard operating environments for each key technology are hardened based on a defined standard, and that standard aligns with:   + Best practice standards (e.g., CIS Benchmarks, STIGs); and/or   + Vendor security guidelines. * Verify that anti-malware protection (such as anti-virus software and/or a next-generation EDR solution) is installed on all systems, and that it is kept up to date. * Confirm for a sample of systems that:   + Anti-malware protection software is installed.   + The anti-malware signatures are up to date (where the technology utilises signatures). |  |  |  |
| **C08** | **Backup and restoration**   * Backups are regularly performed for all systems. * The backup strategy for a system aligns with the recovery objectives established. * Backups are stored in a secure manner. * The ability to restore systems from backups is periodically tested. | DIS.R04 (Moderate)  DIS.R06 (Moderate)  DIS.R10 (High) | **NZISM**  6.4  22.1  **ISO27002**  5.37  8.13  **Rules**  13(1) – 13(5)  13(9) | * Verify that a backup strategy has been documented for each system or group of systems, and that the backup strategy details:   + What data is backed up.   + How often backups are taken.   + How long backups are retained for.   + Where backups are stored. * Verify that the backup strategy considers data stored in cloud systems. * Verify for a sample of systems that the backup strategy is sufficient to meet the established:   + RTO (Recovery Time Objective).   + RPO (Recovery Point Objective). * Confirm that the success of all backup jobs is monitored, and that alerts are automatically generated and escalated for any backup failures. * Review the backup confirmation reports for the past six months and confirm that there is clear evidence of timely follow-up for any backups that failed within that period. * Confirm that restoration testing is performed to formally test the ability to restore from backups when needed. * Review the restoration testing schedule and verify that restoration testing is performed for all systems over a defined cyclic period (that is no longer than three years for any systems). * Verify that backups are appropriately secured (through such mechanisms as encryption and/or physical security controls) to prevent the accidental or unintentional destruction of the backups. |  |  |  |
| **C09** | **Disaster recovery and business continuity planning**   * A formal Disaster Recovery Plan is implemented for each system or group of systems. * The Disaster Recovery Plan(s) is supported by runbooks detailing the step-by-step instructions to recover each system or group of systems. * The Disaster Recovery Plan establishes the recovery timeframes for each system, including:   + The RTO (Recovery Time Objective).   + The RPO (Recovery Point Objective). * The Disaster Recovery Plan is tested on a periodic basis. | DIS.R06 (Moderate)  DIS.R10 (High) | **NZISM**  6.4  **ISO27002**  5.30  **Rules**  13(1) – 13(5)  13(9) | * Verify that a formal Disaster Recovery Plan(s) is in place, and that the plan:   + Has been reviewed within the last 12 months.   + Requires testing of the plan to be performed on at least an annual basis. * Verify that runbooks are established (either within the Disaster Recovery Plan, or as a supplement to it) which detail the steps to follow to recover each system or group of systems. * Verify that the Disaster Recovery Plan(s) has defined RTOs and RPOs for each system or group of systems. * Verify that the Disaster Recovery Plan has been tested within the last year, and that the testing confirmed that the defined RTOs and RPOs were met. |  |  |  |
| **C10** | **Capacity management**   * Capacity thresholds have been established for system resources (such as memory, storage, and CPU usage). * Capacity levels are actively monitored, and remediation activities undertaken where capacity levels go below the established thresholds. | DIS.R10 (High) | **ISO27002**  8.6  **Rules**  13(1) – 13(5) | * Verify that capacity thresholds have been established for system resources, including for:   + Memory usage.   + Storage usage.   + CPU utilisation.   + Network throughput. * Confirm that automated 24x7 monitoring and alerting against the capacity thresholds is in place. * Review the ticketing system (or similar) used to manage any alerts and verify that:   + There are no unactioned alerts.   + All alerts over the past six months were acknowledged within a day, and remediation activities tracked through to closure. |  |  |  |
| **C11** | **Logging**   * All user activity is logged. * Logs are sent off the system to a centralised storage location. * Logs are stored for a reasonable timeframe, and in a manner that prevents them from being altered. * System clocks are synchronised to a standard time source to allow logs to be correlated. | DIS.R01 (High)  DIS.R02 (High)  DIS.R03 (High)  DIS.R05 (Critical)  DIS.R07 (Critical)  DIS.R08 (High)  DIS.R09 (High)  DIS.R10 (High)  DIS.R11 (High) | **NZISM**  16.6  **ISO27002**  8.15  8.17  **Rules**  13(1) – 13(5)  14(6) – 14(7) | * Confirm that a logging standard or policy has been established that:   + Considers logging at an application, operating system, database, and network component level.   + Requires logs are shipped ~~off devices~~ to a centralised location for storage and analysis.   + Details:     - Retention/archival requirements.     - The list of events of be logged.     - How logs are protected.     - The log server availability requirements.     - How reliable delivery of log information to the log server is achieved.   + Requires the following information to be logged (at a minimum):     - All system start-up and shutdown.     - Service, application, component, or system failures.     - Maintenance activities.     - Backup and archival activities.     - System recovery activities.     - Special or out of hours activities.   + Requires the following events to be logged (at a minimum):     - Successful and failed logon attempts.     - All privileged operations.     - Failed attempts to elevate privileges.     - Security related system alerts and failures.     - System user and group additions, deletions, and modification to permissions.     - Unauthorised or failed access attempts to systems and files identified as critical to the organisation.   + Requires the following information to be recorded in the logs:     - Date and time of the event.     - Relevant system user(s) or processes.     - Event description.     - Success or failure of the event.     - Event source (e.g., application name).     - IT equipment location/identification. * Confirm for a sample of systems that the logging implemented aligns with the requirements above. * Verify that logs are retained for at least 18 months. * Verify that an authoritative time source has been established for logging, and that all systems are synchronised with that time source. * Verify how logs are protected from unauthorised access and modification, and from whole or partial loss within the retention period. |  |  |  |
| **C12** | **Security incident management**   * Potential security incidents are monitored 24x7, and any suspicious events escalated for follow-up. * A Security Incident Response Plan is in place to define how the organisation detects, analyses, contains, eradicates, and recovers from security incidents. * The security incident response process is tested on a periodic basis. * An incident register is maintained. * All significant security incidents are reported to:   + Trust Framework Authority.   + Any other organisation required by the Trust Framework Authority. | DIS.R01 (High)  DIS.R02 (High)  DIS.R03 (High)  DIS.R05 (Critical)  DIS.R06 (Moderate)  DIS.R07 (High)  DIS.R08 (High)  DIS.R09 (High)  DIS.R10 (High)  DIS.R11 (High) | **NZISM**  7.1  7.2  7.3  18.4  **ISO27002**  5.24  5.25  5.26  5.27  5.28  8.16  **Rules**  13(1) – 13(5)  13(11) – 13(14) | * Confirm that adequate tools and procedures are implemented to detect potential security incidents, including, for example:   + Tools to monitor system events 24x7 for suspicious or unusual activity, such as:     - A SIEM (Security Incident and Event Management) solution.     - An EDR (Endpoint Detection and Response) solution.     - An IDS (Intrusion Detection System).   + Anti-malware protection – refer control C07.   + Tools to detect the unauthorised egress of data from the environment, such as a DLP (Data Loss Protection) solution.   + System integrity checking tools (such as a data characterisation solution). * Confirm that all staff are made aware of how to report a potential security incident. * Verify that formal guidelines or operating procedures are in place to detail how potential security incidents are escalated. * Confirm that a security incident register is maintained to record and track all identified security incidents, that staff are provided guidance to register security incidents, and that the registers contains the following information (at a minimum) regarding security incidents:   + - Time, date, and country of origin.     - Description of the circumstances.     - Whether the incident was deliberate or accidental.     - An assessment of the degree of compromise or harm.     - A summary of actions taken to resolve the incident. * Confirm that a formal Security Incident Response Plan is established and that it:   + Includes the processes to:     - Detect security incidents.     - Analyse security incidents.     - Contain security incidents.     - Eradicate security incidents.     - Recover from security incidents.   + Is supplemented by runbooks that cover the step-by-step instructions for common types of security incidents.   + Includes (or links to) a communications process to inform stakeholders and keep them up to date.   + Requires the plan to be tested on at least an annual basis.   + Requires the Trust Framework Authority and any other organisation required by the Trust Framework Authority, to be notified of any significant security incidents. * Review the incident register and identify any significant incidents over the past 12 months. Confirm that they have been reported to the Trust Framework Authority and anyone else required by the Trust Framework Authority. * Confirm that the Security Incident Response Plan has been reviewed within the last 12 months. * Confirm that the Security Incident Response Plan has been tested within the last 12 months. |  |  |  |
| **C13** | **Vulnerability management**   * A formal patch management process has been established. * The patch management process considers all technologies and aspects of the systems, including patching of applications, operating systems, databases, and firmware. * Patches are applied in a timely manner following the release of them by vendors. * Where patches cannot be applied, mitigating controls are implemented which reduces the risk posed to a reasonable level. * Vulnerability scanning is regularly performed to identify any potential vulnerabilities or misconfigurations. * Penetration testing is regularly performed to identify any potential vulnerabilities or misconfigurations. * Any vulnerabilities or misconfigurations identified are remediated in a timely manner. They are formally tracked from identification through to remediation. | DIS.R03 (High)  DIS.R05 (High)  DIS.R07 (Critical) | **NZISM**  12.4  **ISO27002**  8.8  **Rules**  13(1) – 13(5)  14(3) | * Confirm that relevant sources for information about new vulnerabilities and security patches (such as vendor vulnerability alerts) are actively monitored. * Verify that the patch management process has been documented, and that it:   + Considers patching at an operating system, application, and firmware level for all system components (not just for operating system patches, for example).   + Considers patching for all technologies used (not just for Microsoft technologies, for example).   + Includes the testing of patches.   + Establishes reasonable timeframes for the remediation of vulnerabilities (e.g., for the application of patches following their release).   + Requires all critical patches to be applied within two days of release.   + Contains a structured approach to evaluate and approve the implementation of mitigating controls when a patch is not available or cannot be installed.   + Includes monthly reporting of the patch status of systems. * Confirm that vulnerability scanning is performed for all systems components on at least a monthly basis. * Confirm that independent penetration testing is performed on at least an annual basis. * Obtain the most recent patch report and verify that:   + The patch status of all technologies and systems components are considered.   + Patches are being applied in a timely manner in line with the remediation timelines established (and if not, there were reasonable explanations to why not, and the risk posed by this was documented and escalated). * Review the reports from the most recent vulnerability scanning and penetration testing and verify that:   + The testing was comprehensive.   + The type of vulnerability scanning tools used aligned with what was being tested e.g., that a web vulnerability scanner was using for testing web-based applications.   + Any findings identified are recorded in a centralised register, where they are tracked through to remediation.   + The findings were remediated or mitigated within the established timeframes (and if not, there were reasonable explanations to why not, and the risk posed by this was documented and escalated).   + The risk acceptance of any findings appears reasonable. |  |  |  |
| **C14** | **Denial-of-service protection**   * Robust vulnerability management processes are in place to reduce the likelihood of a denial of service (DoS) attack being successful. * A denial of service (DoS) response plan is in place to help the organisation respond to any denial of service. * Distributed Denial of Service (DDoS) protection is in place for all Internet facing components to minimise the likelihood of distributed denial-of-service attack being successful. | DIS.R06 (Moderate) | **NZISM**  18.3  **Rules**  13(1) – 13(5) | * Verify that robust vulnerability management processes are in place – *refer C13.* * Verify that a denial-of-service response plan has been documented, and that the plan includes:   + How to identify the precursors and other signs of DoS.   + How to diagnose the incident or attack type and attack method.   + How to diagnose the source of the DoS.   + What actions can be taken to clear the DoS.   + How communications can be maintained during a DoS.   + Reporting requirements. * Confirm that denial of service response plan includes monitoring and use of such aspects as:   + Router and switch logging and flow data.   + Packet captures.   + Proxy and call manager logs and access control lists.   + Video & Telephony Conferencing (VTC) and IPT aware firewalls and voice gateways.   + Network redundancy.   + Load balancing.   + PSTN failover.   + Alternative communication paths. * Confirm that a DDoS mitigation service is in place to mitigate the impact of any DDoS attacks on Internet facing system components. |  |  |  |
| **C15** | **Asset management**   * A formal asset management process is established to manage the end-to-end lifecycle of assets. * All hardware and software assets are recorded in asset registers. * The asset registers are kept up to date. * Unsupported software is not used. * All data is securely deleted ~~of~~ when assets are disposed of. | DIS.R04 (Moderate)  DIS.R07 (Critical) | **NZISM**  8.4  12.6  13.4  **ISO27002**  5.9  7.10  7.14  **Rules**  13(1) – 13(5)  14(4) | * Confirm that a formal asset management process is in place to manage the end-to-end lifecycle of an asset, including the security requirements to:   + Purchase or develop an asset.   + Repurpose an asset.   + Dispose of an asset. * Confirm that the asset management process considers at least hardware and software assets. * Confirm that processes are established to keep the asset registers up to date, such as:   + Integration with the change management process.   + The use of asset discovery software. * Review the software asset register and verify that there are no unsupported operating systems, applications, or other software in use. * Verify that there is integration between the asset management processes and the vulnerability management processes to ensure that:   + All systems are being considered in the vulnerability management processes e.g., vulnerability scanning is being performed for all systems.   + The asset registers are kept up to date (with information such as software versions). * Confirm that a formal data destruction process is in place, and that the process requires:   + The archiving of data in line with the established data retention policy.   + The sanitisation or destruction of any media before equipment is disposed of.   + That formal authorisation is obtained before the sanitisation or destruction of the media.   + Verification of the sanitisation of media or IT equipment is done using a different product from the one used to perform the initial sanitisation.   + For non-volatile media (such as hard disks), the media is sanitised by:     - Overwriting the media at least once in its entirety with an arbitrary pattern followed by a read back for verification.     - Booting from separate media to the media being sanitised.     - Resetting the host protected area and drive configuration overlay table of non-volatile magnetic hard disks prior to overwriting the media.     - Attempting to overwrite the growth defects table (g-list).     - Using the ATA security erase command for magnetic hard disks instead of using block overwriting software.   + For solid state drives:     - The drives are destroyed before disposal.     - Sanitised using ATA Secure Erase sanitation software before redeployment.   + For hybrid drives (if relevant):     - The drives be treated in the same way as solid state drives.   + For any printers (if relevant):     - At least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum.     - The cartridge or drum is destroyed where the printer cartridges with integrated copier drums or discrete copier drums cannot be sanitised.   + For any CRT televisions and monitors (if relevant):     - The screens are inspected turning up the brightness to the maximum level to determine if any information has been burnt into or persists on the screen.   + For the following (if relevant), they are destroyed rather than disposed of:     - Optical discs.     - Printer ribbons and the impact surface facing the platen.     - Programmable read-only memory (PROM, EPROM, EEPROM).     - Flash memory and solid state or hybrid data storage devices.     - Read-only memory.     - Faulty magnetic media that cannot be successfully sanitised.   + For volatile media (if relevant), the media is sanitised by:     - Overwriting all locations of the media with an arbitrary pattern.     - Followed by a read back for verification.     - Removing power from the media for at least 10 minutes.   + For non-volatile EPROM media (if relevant) by:     - Erasing as per the manufacturer’s specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.   + For non-volatile EEPROM media by:     - Overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.   + For non-volatile flash memory (if relevant) by:     - Overwriting the media at least twice in its entirety with a pseudo random pattern, followed by a read back for verification.   + That where media is destroyed rather than sanitised:     - Any incineration equipment used by the facility performing the destruction is rated for the destruction of electronic waste (WEEE) and the operator is properly authorised or licensed.     - The facility performing the destruction has processes in place for the safe handling of electronic waste (WEEE), including any residual material from the destruction process.     - A degausser of sufficient field strength for the coercivity of the media or IT equipment.     - The degausser which has been evaluated as capable for the magnetic orientation (longitudinal or perpendicular) of the media.     - Product specific directions provided by the manufacturers must be followed.     - The destruction of the media and IT equipment is performed under the supervision of at least one person.     - Personnel supervising the destruction of media or IT equipment must supervise the handling of the media or IT equipment to the point of destruction, and ensure that the destruction is completed successfully.     - The destruction register records the destruction facility used, destruction method used, date of destruction, operator and witness, media and IT equipment type, characteristics and serial number. * Inspect the asset register ~~and~~ for a sample of IT equipment or media that has been disposed of in the past 12 months and verify through review of the disposal register that data has been securely disposed of in accordance with the expectations above. |  |  |  |
| **C16** | **Human resource security**   * Staff are provided regular security awareness training. * Security vetting is performed for staff. * The ongoing suitability of staff is assessed. * Staff members are made aware of the organisation’s security policies and standards, along with their role and responsibilities for maintaining security. | DIS.R01 (High) | **NZISM**  9.1  **ISO27002**  6.1  6.2  6.3  **Rules**  13(1) – 13(5)  16 | * Confirm that security vetting is performed on all staff, including:   + Employees.   + Contractors.   + Third-party support provider staff.   Where services are delivered by third-party support provider staff, their employer may perform the vetting. In those situations, only confirmation that it has been completed without issues would be needed, rather than it needing to be reperformed.   * Confirm that the vetting process includes performing criminal record checks. * Confirm that the vetting process considers the ongoing suitability of staff. * Confirm that security awareness training takes place when all relevant staff (including contractors) initially join the organisation, and then on an ongoing basis once joined. * Confirm that a structured process is in place to follow-up on any staff who have not completed the security awareness training in the timeframes expected. * Verify for a sample of new starters during the past year that they have completed their security training as expected through inspecting the training records. * Confirm that all staff (including contractors and third-party support provider staff) are made aware of the organisation’s security policies and standards, along with their responsibilities for maintaining cyber security, through:   + The security policies and standards being made readily available e.g. through publishing on the intranet.   + Staff being made aware of the security policies and standards as part of the security awareness training provided.   + Staff with specific security roles having their responsibilities outlined within their position descriptions or contracts.   + The contracts with third-party support providers detailing the organisation’s expectations for managing security. |  |  |  |
| **C17** | **Third-party risk management**   * All third parties with access to the systems or data are clearly identified (including any cloud providers). * The security risks posed by third-party organisations (including cloud providers) are assessed before onboarding a third-party, and then on an ongoing basis. | DIS.R01 (High)  DIS.R02 (High)  DIS.R03 (High)  DIS.R04 (Moderate)  DIS.R05 (High)  DIS.R06 (High)  DIS.R07 (High)  DIS.R08 (High)  DIS.R09 (High)  DIS.R10 (High)  DIS.R11 (High) | **NZISM**  **22.1**  **ISO27002**  5.19  5.20  5.21  5.22  **Rules**  13(1) – 13(5) | * Verify that a formal third-party security risk management process is in place to manage the security risks posed by third party organisations, including cloud providers. * Confirm that the third-party security risk management process includes steps to:   + Ensure appropriate security related clauses are included in contracts.   + Assess the security risks and appropriateness of the controls implemented before a new third-party provider is onboarded.   + Re-assess the security risks and controls on an ongoing cyclic basis. * Verify that a register (or similar) of third-party providers is maintained, and that there are processes in place to ensure that it is kept up to date. * For a sample of existing third-party providers, verify that the security risks and controls were re-assessed in line with a defined schedule (and no more than three years since they were last assessed). * For a sample of new third-party providers over the past year, verify that the security risks and controls were assessed and deemed to be within the organisation’s security risk appetite. |  |  |  |
| **C18** | **Physical and environmental security**   * Physical access to the infrastructure delivering the identity services is restricted to those individuals that require physical access to undertake their roles. * The user access reviews performed include reviews over access to secure locations (e.g., data centres, server rooms, communication cupboards) used to deliver the services. * Mechanisms are in place to achieve resilience requirements in normal or adverse situations, for example backup generators and alternate telecommunications services. * Environmental controls are implemented to protect against environmental threats such as fire, flooding, and extreme temperatures. Environmental conditions are actively monitored and automatically escalated when outside of established parameters. | DIS.R01 (High)  DIS.R06 (Moderate)  DIS.R08 (High)  DIS.R09 (High) | **NZISM** 8.1  8.2  8.3  **ISO27002**  7.1  7.2  7.3  7.4  7.5  7.6  7.8  **Rules**  13(1) – 13(5)  15 | * For any data centres, server rooms, patch cupboards, or other similar locations where IT equipment delivering the services is located, verify through walkthrough and inspection that the access controls in place sufficiently control access to the locations. * Verify that the user access reviews performed (in line with C01) include access to physical locations, through inspecting the report from the last review performed. * For any data centres or server rooms, verify that resilience mechanisms (such as backup generators and alternative telecommunications service) are:   + In place.   + Maintained in line with a defined maintenance plan. * Verify through walkthrough and inspection that environmental controls are implemented to protect against environmental threats. * Confirm that environmental conditions are actively monitored, and that any alerts are raised and actioned upon. |  |  |  |
| **C19** | **Network security**   * Network segregation is implemented to segregate different security domains e.g.:   + The systems providing identity services from the organisation’s corporate systems.   + Non-production systems from production systems. * Jump hosts or dedicated privileged access workstations are used to access the network segments containing the systems delivering identity services. * Multi-factor authentication is used to move between security segments. * The firewalls used to segregate the network are managed from an isolated management network, or from the higher of the security domains that they segregated. * Any external facing websites, web-based applications or APIs used to deliver the identity services are protected by a web application firewall (or similar application gateway). | DIS.R01 (High)  DIS.R05 (High)  DIS.R07 (High) | **NZISM**  10.8  22.2  **ISO27002**  8.20  8.21  8.22  **Rules**  13(1) – 13(5) | * Confirm that network segregation is implemented between different security domains e.g.:   + The systems providing identity services from the organisation’s corporate systems.   + Non-production systems from production systems. * Confirm that segregation between domains is not achieved using virtualisation technology. * Verify the network segregation in place through reviewing network diagrams or firewall architectures. * Confirm that administrators access the environment(s) providing the identity services via jump hosts or dedicated privilege access workstations. * Verify that multi-factor authentication is used to move between security domains. * Verify through inspection of the network diagrams or firewall architectures that the firewalls used to segregate the network segments are managed from either:   + An isolated management network; or   + The higher of the security domains. * Verify through reviewing the report from the last penetration test performed:   + That the scope of the testing included testing network segregation.   + That there were no issues identified relating to network segregation.   + That there were no issues identified in relation to the configuration (or absence) of the web application firewall. |  |  |  |
| **C20** | **Security assurance**   * A structured security assurance programme is in place to validate the ongoing effectiveness of the key security controls. * Security testing is performed by independent people. * The security of any new systems is tested before being placed into production. | DIS.R01 (High)  DIS.R02 (High) DIS.R03 (High)  DIS.R05 (High)  DIS.R06 (High)  DIS.R07 (High)  DIS.R08 (High)  DIS.R09 (High)  DIS.R10 (High)  DIS.R11 (High) | **NZISM**  6.1  6.2  **ISO27002**  5.35  5.36  **Rules**  13(1) – 13(5) | * Verify that a structured annual programme of work is in place to validate the design and operating effectiveness of the key security controls in place.   This may include such testing as:   * + Internal-audit reviews.   + Third-party reviews.   + Continuous assurance processes.   + Penetration tests – *refer C13.*   + Vulnerability scanning – *refer C13*.   Note that penetration testing and vulnerability scanning alone will not provide sufficient coverage of all the key controls.   * Confirm that the assurance programme addresses physical security as well as logical security. * Confirm that the people responsible for performing the different assurance activities are independent to those responsible for designing and operating the key controls. * Confirm that security testing is performed for any new systems before they are placed into production, or after any significant change. * Review the reports from the assurance activities performed over the past year and verify that:   + The assurance activities covered all the key controls.   + The results of the testing support the conclusions reached for the other controls in the Controls Validation Plan.   + Any issues identified were documented and tracked through to remediation (or the risk accepted by an appropriate person, following a structured risk acceptance process). |  |  |  |
| **C21** | **Security risk management**   * A security risk assessment has been completed for the service to help inform decisions around security. * The security risk assessment is updated on a periodic basis to assess the impact of evolving threats. * The security risk management process is supported by a threat management process to ensure the security measures continue to be fit for purpose. | N/A | **NZISM**  5.3  **Rules**  13(1) – 13(5) | * Verify that a security risk assessment has been performed for the service within the past 12 months. * Confirm that:   + The structure of the security risk assessment aligns with generally accepted practices (as outlined in the likes of ISO 31000 and ISO 27005) and includes assessments and mitigations for the following risks at a minimum:     - Weak human resource security.     - Insufficient incident response.     - Insecure facilitation mechanism.     - Credential loss due to device or facilitation. mechanism failure.     - Insecure API endpoints.     - Service provider outage.     - Compromise of trust framework provider infrastructure.     - Security of hosting services.     - Weak service provider access controls.     - Credentials unable to be verified.     - Unauthorised usage of valid credentials.   + The risk assessment considers the identified information and systems regarding their value, importance, and sensitivity.   + The risk assessment considers physical security as well as logical security.   + All the risks are within the organisation’s security risk appetite, with none of the risks having a significant residual risk (e.g. major/high rating). * Confirm that a structured threat management process is followed to help inform the risks in the security risk assessment, and to ensure that the security risk assessment takes into account the evolving threat environment. |  |  |  |

# Risk evaluation guidelines

1. Completing a controls validation

2.Conducting a risk evaluation

3. Identifying the security risk position

4. Confirming findings and remediations

5. Documenting information used and additional evidence

## Introduction

The gross risk ratings (the risk ratings with no controls in place) have been determined by the Trust Framework Authority. The acceptable risk rating has also been calculated. This is the minimum acceptable risk for accredited digital identity services.

The independent evaluator must evaluate the risk once the relevant controls are in place (the assessed risk). The assessed risk is calculated by evaluating the likelihood and impact of the risk occurring, given the controls in place to mitigate the risk, and then using the risk matrix to provide the overall assessed risk position.

If providers do not reach the acceptable risk rating, they 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 risk evaluation

**Table 3 – Risk evaluation components**

| **Component** | **Description** |
| --- | --- |
| Risk ID | The identification number for the risk. |
| Risk description | The description of the risk. |
| Expected controls | The controls that are expected to be in place by the provider to mitigate against the risk. |
| Gross risk | The risk rating with no risk treatment (controls) in place. These have been calculated by the Trust Framework Authority and the same gross risk rating will apply for all providers. |
| Acceptable risk | The minimum level of risk that is acceptable for accredited providers. |
| Assessed risk | The level of risk evaluated by the independent evaluator once the expected controls for the risk are in place. This is the risk remaining after the risk treatment has been applied. |
| Likelihood | The likelihood of the risk occurring. This is calculated by identifying the level of difficulty in exploiting the vulnerability. The scale includes almost certain, highly probably, possible, possible but unlikely, almost never. This is set out in **Table 4**. |
| Impact | The impact of the risk occurring. This is a scale showing the possible consequences of the identified risks, including cascade and cumulative effects. The scale includes severe, significant, moderate, minor and minimal. This is set out in **Table 5**. |
| Risk rating | The overall risk rating given the likelihood and impact of the risk. This is ascertained by looking at the appropriate cell in the risk rating table. This is set out in **Table 6.** |
| Risk evaluation | The independent evaluator’s recording of the rationale for their rating. |

**Likelihood (probability) evaluation**

The qualitative scale used to assign a likelihood rating is presented in **Table 4** below. Where information is available about the frequency of an incident in the past it may be used to determine the likelihood of the risk eventuating. However, where such information does not exist it does not necessarily mean that the likelihood of the risk eventuating is low. It may merely indicate that there are no controls in place to detect it or that the provider has not previously been exposed to the particular risk.

**Table 4 – Risk likelihood scale**

| **Rating** | **Description** | **Meaning** |
| --- | --- | --- |
| 5 | Almost certain | It is easy for the threat to exploit the vulnerability without any specialist skills or resources or it is expected to occur within 1 – 6 months. |
| 4 | Highly probable | It is feasible for the threat to exploit the vulnerability with minimal skills or resources or it is expected to occur within 6 – 12 months. |
| 3 | Possible | It is feasible for the threat to exploit the vulnerability with moderate skills or resources or it is expected to occur within 12 – 36 months. |
| 2 | Possible but unlikely | It is feasible but would require significant skills or resources for the threat to exploit the vulnerability or it is expected to occur within 3 – 5 years. |
| 1 | Almost never | It is difficult for the threat to exploit the vulnerability or it is not expected to occur within 5 years. |

### Impact evaluation

The qualitative scale used to assign an impact rating is presented in **Table 5**. The impact of risks includes consideration of any possible repercussions of the consequences of the identified risks, including cascade and cumulative effects.

**Table 5 – Impact evaluation**

| **Rating** | **Description** | **Impact** |
| --- | --- | --- |
| **5** | **Severe** | * A significant number of users are subject to identity theft. * Major reduction of usage and uptake of digital identity services. * Major loss of trust from relying parties utilising digital identity services for verification. * Major loss of trust from the public. * The Trust Framework Provider suffers severe reputational damage. * Media interest is sustained for a prolonged period (i.e., over a week) with major criticism levelled at the provider. * External investigation into the incident is expected. * Impact cannot be managed without significant extra human resources. * Major additional financial resources are required for investigation, incident response and compensation. |
| **4** | **Significant** | * Many users are subject to identity theft. * Significant reduction of usage and uptake of digital identity services. * Significant loss of trust from relying parties utilising digital identity services for verification. * Significant loss of trust from the public. * The Trust Framework Provider suffers significant reputational damage. * Media interest is sustained for up to a week with criticism levelled at the provider. * External investigation into the incident is expected. * Impact cannot be managed without re-prioritisation of work programmes. * Significant additional financial resources are required for investigation, incident response and compensation. |
| **3** | **Moderate** | * A limited number of users are subject to identity theft. * Moderate reduction in usage and uptake of digital identity services. * Moderate loss of trust from relying parties utilising digital identity services for verification. * Moderate loss of trust from the public. * The Trust Framework Provider suffers limited reputational damage. * Media interest is sustained for less than a week with criticism levelled at the provider. * Internal investigation is commissioned by the provider. * Impact can be managed with some re-planning and modest extra financial or human resources. * Some additional financial resources are required for investigation, incident response and compensation. |
| **2** | **Minor** | * A moderate number of users have a limited set of identity information disclosed. * Loss of trust in digital identity services from impacted people. * Slight reduction in uptake and usage of digital identity services. * Senior management and stakeholders believe that the Trust Framework Authority’s reputation has been damaged. * Media interest is short-lived (i.e., a couple of days) and a small amount of blame is directed at the provider. * Communications and recovery can be managed internally. * Impact can be managed within current resources, with some re-planning. * Limited additional financial cost. |
| **1** | **Minimal** | * A small number/individual has a limited amount of identity information disclosed. * Minor reduction in trust of digital identity services from impacted users. * No reduction of uptake of digital identity services. * The Trust Framework Provider’s reputation is unaffected. * Limited to no media attention. * All communications and recovery can be managed internally. * Limited additional financial cost. |

### Risk rating

The overall risk rating given the likelihood and impact of the risk. For example, if a risk had a likelihood of possible and impact of moderate, it would have an overall risk rating of 13 (High).

**Table 6 – Risk rating**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Impact** | **Severe** | **15** | **19** | **22** | **24** | **25** |
| **Significant** | **10** | **14** | **18** | **21** | **23** |
| **Moderate** | **6** | **9** | **13** | **17** | **20** |
| **Minor** | **3** | **5** | **8** | **12** | **16** |
| **Minimal** | **1** | **2** | **4** | **7** | **11** |
|  | | **Almost never** | **Possible but unlikely** | **Possible** | **Highly probable** | **Almost certain** |
| **Likelihood** | | | | |

Risks are classified as follows:

* Zone 4/Critical (risks 22, 23, 24 and 25, shown in red).
* Zone 3/High (risks 14 – 20, shown in orange).
* Zone 2/Moderate (risks 4 – 13, shown in yellow).
* Zone 1/Low (risks 1 -3, shown in green).

# Risk evaluation

| Risk ID | Risk description | Expected controls | Acceptable risk | | | Assessed risk | | | Risk evaluation |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Impact | Risk rating | Likelihood | Impact | Risk rating |  |
| **R01** | **Staff member causes breach**  A provider’s environment is intentionally or unintentionally compromised by a staff member. This may be due to weak security awareness training or security vetting, and may lead to an information breach, modification, loss, or system outages.  This risk applies to the following services:   * Binding service. * Authentication service. * Information service. * Credential service. * Facilitation service. | * C01 – User Access Management * C02 – Authentication * C11 – Logging * C12 – Security Incident Management * C16 – Human Resource Security * C17 – Third Party Risk Management * C18 – Physical and Environmental Security * C19 – Network Security * C20 – Security Assurance | Almost Never | Moderate | Zone 2 (6) |  |  |  |  |
| **R02** | **Insufficient incident response**  A security incident occurs at a Trust Framework Provider which is not responded to in a timely and effective manner. This may be due to weak monitoring or incident response processes, and may lead to an information breach, modification, loss, or system outages.  This risk applies to the following services:   * Binding service. * Information service. * Credential service. * Authentication service. * Facilitation service. | * C11 – Logging * C12 – Security Incident Management * C17 – Third Party Risk Management * C20 – Security Assurance | Possible | Minor | Zone 2 (8) |  |  |  |  |
| **R03** | **Insecure digital identity facilitation mechanism**  A digital identity facilitation mechanism, such as a wallet, is compromised due to vulnerabilities being present within its source code. This may be due to insecure development practices, and may lead to an information breach, modification or loss.  This risk applies to the following services:   * Facilitation service. | * C05 – Secure Systems Development * C06 – Change Management * C11 – Logging * C12 – Security Incident Management * C14 – Vulnerability Management * C17 – Third Party Risk Management * C20 – Security Assurance | Possible but Unlikely | Minor | Zone 2 (5) |  |  |  |  |
| **R04** | **Credential loss due to device or facilitation mechanism (e.g. wallet) failure**  A digital identity facilitation mechanism (for example a wallet) is no longer accessible due to the device it was held on being lost or destroyed. Therefore, the credentials within the facilitation mechanism are no longer usable. If credentials are unable to be securely re-generated or migrated within a reasonable time, a user may be left with no digital credentials and not be able to access services they require.  This risk applies to the following services:   * Authentication service. * Facilitation service. * Credential service. | * C06 – Change Management * C08 – Backup and Restoration * C15 – Asset Management * C17 – Third Party Risk Management | Possible | Minor | Zone 2 (8) |  |  |  |  |
| **R05** | **Insecure API endpoints**  An API endpoint that is used by a digital identity service is compromised due to an insecure authentication or authorisation mechanism having been implemented. This may lead to unauthorised access to or modification of personal information.  This risk applies to the following services:   * Binding service * Information service * Credential service * Authentication service. * Facilitation service. | * C01 – User Access Management * C02 – Authentication * C04 – Encryption * C05 – Secure Systems Development * C11 – Logging * C12 – Security Incident Management * C13 – Vulnerability Management * C17 – Third Party Risk Management * C19 – Network Security * C20 – Security Assurance | Possible | Moderate | Zone 2 (13) |  |  |  |  |
| **R06** | **Provider outage**  A disaster or large duration outage occurs, causing disruptions at a Trust Framework Provider. The provider is not able to maintain or restore its services in a reasonable amount of time. This may lead to prolonged service outages.  This risk applies to the following services:   * Binding service. * Authentication service. * Information service. * Credential service. * Facilitation service. | * C06 – Change Management * C08 – Backup and Restoration * C09 – Disaster Recovery Planning * C12 – Security Incident Management * C14 – Denial-of-Service Protection * C17 – Third Party Risk Management * C18 – Physical and Environmental Security * C20 – Security Assurance | Almost Never | Minor | Zone 1 (3) |  |  |  |  |
| **R07** | **Compromise of provider infrastructure**  A provider’s infrastructure is compromised due to inadequate host maintenance, patching, updating or hardening. This may lead to an information breach, modification, loss, or system outages.  This risk applies to the following services:   * Binding service. * Authentication service. * Information service. * Credential service. * Facilitation service. | * C06 – Change Management * C07 – Host Protection * C11 – Logging * C12 – Security Incident Management * C13 – Vulnerability Management * C15 – Asset Management * C17 – Third Party Risk Management * C19 – Network Security * C20 – Security Assurance | Possible but Unlikely | Moderate | Zone 2 (9) |  |  |  |  |
| **R08** | **Security of hosting services**  A provider is compromised due to a data centre breach, or compromise of their cloud service provider. This may lead to an information breach, modification, loss, or system outages.  This risk applies to the following services:   * Binding service. * Authentication service. * Information service. * Credential service. * Facilitation service. | * C11 – Logging * C12 – Security Incident Management * C17 – Third Party Risk Management * C18 – Physical and Environmental Security * C20 – Security Assurance | Possible but Unlikely | Minor | Zone 2 (5) |  |  |  |  |
| **R09** | **Weak provider access controls**  Technology components that deliver a digital identity service and protect its data are compromised due to weak access controls. This may lead to an information breach, modification, loss, or system outages.  This risk applies to the following services:   * Binding service. * Authentication service. * Information service. * Credential service. * Facilitation service. | * C01 – User Access Management * C02 – Authentication * C03 – Privileged Access Management * C11 – Logging * C12 – Security Incident Management * C17 – Third Party Risk Management * C18 – Physical and Environmental Security * C20 – Security Assurance | Possible but Unlikely | Moderate | Zone 2 (9) |  |  |  |  |
| **R10** | **Credentials unable to be verified**  The mechanism used to verify credentials for authenticity expires or becomes unavailable due to inappropriate management. This leads to user credentials being unable to be verified.  Example scenarios:   * A certificate used to verify the authenticity of a widely used credential expires, invalidating many valid credentials. * A key authentication provider has an outage, disrupting the issuance of new credentials. * An administrator fails to follow appropriate standard operating procedures and does not renew a certificate in time, leading to credentials becoming unverifiable.   This risk applies to the following services:   * Credential service. * Authentication service. * Facilitation service. | * C04 –Encryption * C06 – Change Management * C08 – Backup and Restoration * C09 – Disaster Recovery Planning * C11 – Logging * C12 – Security Incident Management * C10 – Capacity Management * C17 – Third Party Risk Management * C20 – Security Assurance | Possible but Unlikely | Minor | Zone 2 (5) |  |  |  |  |
| **R11** | **Unauthorised usage of valid credentials**  A facilitation mechanism holding digital identity credentials is maliciously or accidently used by an unauthorised person. This may be due to insecure access controls to secure the facilitation mechanism and it may lead to the misuse of digital credentials and theft of identity.  This risk applies to the following services:   * Facilitation service. * Authentication service. | * C01 – User Access Management * C02 – Authentication * C04 – Encryption * C11 – Logging * C12 – Security Incident Management * C17 – Third Party Risk Management * C20 – Security Assurance | Possible | Moderate | Zone 2 (9) |  |  |  |  |

# Security risk position

Based on the outcome of the evaluation, the evaluator has made the following determination on the **assessed risk position** of the digital identity service.

Map each risk by recording it in the relevant square of the table, using the assessed likelihood and impact for each risk.

**Table 7 Assessed risk rating**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Impact** | **Severe** | **15** | **19** | **22** | **24** | **25** |
| **Significant** | **10** | **14** | **18** | **21** | **23** |
| **Moderate** | **6** | **9** | **13** | **17** | **20** |
| **Minor** | **3** | **5** | **8** | **12** | **16** |
| **Minimal** | **1** | **2** | **4** | **7** | **11** |
|  | | **Almost never** | **Possible but unlikely** | **Possible** | **Highly probable** | **Almost certain** |
| **Likelihood** | | | | |

# Findings and remediations

1. Completing a controls validation

2.Conducting a risk evaluation

3. Identifying the security risk position

4. Confirming findings and remediations

5. Documenting information used and additional evidence

Only findings that require mediation for the control to be effective should be listed here. If a finding requires remediation to achieve an acceptable level of risk, 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:

| **Finding ID** | **Finding** | **Associated controls** | **Planned mitigations** | **Planned mitigation date** | **Status** |
| --- | --- | --- | --- | --- | --- |
| F01 |  |  |  |  | Open/ Resolved/ In-Progress/ Compensating Controls Applied |
| F02 |  |  |  |  |  |
| F03 |  |  |  |  |  |
| F04 |  |  |  |  |  |

# Information and additional evidence used to inform your evaluation

1. Completing a controls validation

2.Conducting a risk evaluation

3. Identifying the security risk position

4. Confirming findings and remediations

5. Documenting information used and additional evidence

The following documents were reviewed to inform this security evaluation:

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

The following interviews, observations and visits were held to inform this security 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 - Risks applicable for each Digital Identity Service

### Risks applicable for each Digital Identity Service

| **Risk** | **Digital identity Service** | | | | |
| --- | --- | --- | --- | --- | --- |
| **Credential** | **Facilitation** | **Authentication** | **Information** | **Binding** |
| R01 Staff member causes breach | ü | ü | ü | ü | ü |
| R02 Insufficient incident response | ü | ü | ü | ü | ü |
| R03 Insecure digital identity facilitation mechanism |  | ü |  |  |  |
| R04 Credential loss due to device or facilitation mechanism (e.g. wallet) failure | ü | ü | ü |  |  |
| R05 Insecure API endpoints | ü | ü | ü | ü | ü |
| R06 Provider outage | ü | ü | ü | ü | ü |
| R07 Compromise of provider infrastructure | ü | ü | ü | ü | ü |
| R08 Security of hosting services | ü | ü | ü | ü | ü |
| R09 Weak provider access controls | ü | ü | ü | ü | ü |
| R10 Credentials unable to be verified | ü | ü | ü |  |  |
| R11 Unauthorised usage of valid credentials |  | ü | ü |  |  |

Appendix B - Glossary

| **Term** | **Definition** |
| --- | --- |
| API | An Application Programming Interface (API) is a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service. |
| Assessed risk | The risk remaining after the risk treatment has been applied. |
| Authentication service | A service that enables a user to use an authenticator to access a service, for example a log-in service or a 2–factor authentication service. |
| Authenticator | Means information or another thing, for example a password, a personal identification number, or a fingerprint, that:   1. Is known to, or possessed or controlled by, a person; and. 2. Is bound or otherwise linked to the user during an interaction with a service; and 3. Can be used by the person during subsequent interactions with the service to prove the user is the same person. |
| Bind | In relation to personal or organisational information, means to link securely to the correct individual or organisation by means of one or more checks that the information relates to that particular individual or organisation. |
| Binding service | A service that binds personal or organisational information. |
| Consequence | The outcome of an event. The outcome can be positive or negative. However, in the context of information security it is usually negative. |
| Control | A risk treatment implemented to reduce the likelihood and/or impact of a risk. |
| Credential | A digital record of bound personal or organisational information, for example a digital vaccination record, that can be:   1. Accepted by a relying party or another person as being valid without further verification of the information itself. 2. Relied on by a relying party or another person. |
| Credential service | A service that creates a reusable credential. |
| Facilitation | Means the processes that support users to claim, hold and manage their credentials, and to present their credentials to relying parties. |
| Facilitation mechanism | Means a product that can facilitate the presentation of one or more credentials (fully or partially) in response to a request from a relying party. Examples include digital wallets. |
| Facilitation service | A service that uses a facilitation mechanism to enable a person to present a credential to a relying party. |
| Gross risk | The risk without any risk treatment applied. |
| Impact | See Consequence. |
| Information Security | Ensures that information is protected against unauthorised access or disclosure (confidentiality), or unauthorised or improper modification (integrity), and can be accessed when required (availability). |
| Likelihood/ Probability | The chance of an event occurring. |
| Recovery Point Objective (RPO) | The maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or other event before data loss will exceed what is acceptable to the organisation. |
| Recovery Time Objective (RTO) | The amount of time allowed for the recovery of an information system or service after a disaster event has occurred. The RTO effectively specifies the amount of time that is acceptable to the business to be without the system. |
| Relying party | An individual who, or an organisation that, relies on personal or organisational information shared, in a transaction with a user, through one or more digital identity services. |
| Risk | The effect of uncertainty on objectives. |
| Risk owner | A person or entity with the accountability and authority to manage a risk. |
| Stakeholder | A person or organisation that can affect, be affected by, or perceive themselves to be affected by, a risk eventuating. |
| Subject | A person or an organisation that is the focus of personal or organisational information. |
| 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 |
| Threat | A potential cause of a risk. |
| User | An individual who:  shares personal or organisational information, in a transaction with a relying party, through one or more accredited digital identity services; and  does so for themselves or on behalf of another individual or an organisation. |
| Vulnerability | A weakness in an information system or service that can be exploited by a threat. |

1. https://nzism.gcsb.govt.nz/ [↑](#footnote-ref-2)
2. https://www.iso.org/standard/75652.html [↑](#footnote-ref-3)