**Conformance Workbook – Credential establishment Assurance**

This workbook outlines the evidence that needs to be provided to the Assessor for them to audit conformance with Part 1 - Requirements for Credential Providers establishing Credentials of the Federation Assurance Standard (effective 1 October 2024).

Each piece of evidence is given a code. Where the evidence can be used for multiple controls, it will retain the same code.

**Checklist of evidence needed for a conformance audit**

The following checklist provides a summary of the evidence needed in preparation for an audited assessment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Check** | **Evidence** |  | **Met/Not Met** | **Assessment notes** |
|  | AUDIT1.1 – Completed Identification Risk Assessment/s  or AUDIT1.2 |  |  |  |
|  | (only needed if AUDIT1.1 not used)  AUDIT1.2 – Other risk assessment based on ISO31000 |  |  |  |
|  | AUDIT1.4 – Privacy Impact Assessment containing:   1. information about use of the Entity Information identifier (IPP13), 2. information about the disclosure of information during Credential presentation (IPP11). |  |  |  |
|  | AUDIT3.1 – Credential Management document **(or equivalent)** containing:   1. a rationale for selected level of Authenticator and Authenticator type/s to be used, 2. information about the method/s for declaring levels, 3. detailed information about the technologies and techniques used to ensure authenticity and uniqueness of the Credential, 4. detailed information that describes technologies and techniques used to ensure the recognition and authenticity of Credential Provider, 5. a description of the application process and how it meets the population needs, 6. details about the Credential holders’ ability to manage their Credential, 7. information about complaints handling, 8. Credential status management procedures, 9. information about system logging and monitoring. |  |  |  |
|  | AUDIT3.2 – Identification Standards conformance certificate/s |  |  |  |
|  |  |  |  |  |

**Controls and the audit evidence**

The following tables lists the controls and the Audit evidence applicable to each.

**Federation Assurance Controls**

|  |  |  |
| --- | --- | --- |
| **Reference** | **Objective/Control description** | **Audit evidence/criteria** |
| ***Objective 1*** | ***Credential risk is understood*** |  |
| FA1.01 | The CP MUST carry out an assessment of the risk posed by the existence of the Credential before offering it. | AUDIT1.1 – Completed Identification Risk Assessment/s  or AUDIT1.2 – Other risk assessment based on ISO31000 |
| FA1.02 | The CP MUST evaluate the risk of all information available to a holder viewing or managing their Credential and apply the corresponding level of authentication. | AUDIT1.1 – Completed Identification Risk Assessment/s or AUDIT1.2 – Other risk assessment based on ISO31000  AUDIT3.1a – Credential Management document (or equivalent) containing rationale for selected level of Authenticator and Authenticator type/s to be used. |
| ***Objective 2*** | ***Credentials have recognised levels of assurance*** |  |
| FA2.01 | The CP MUST establish the Credential using identification processes that comply with the latest versions of the following standards:  • Information Assurance Standard  • Binding Assurance Standard  • Authentication Assurance Standard. | AUDIT3.2 – Identification Standards conformance certificate/s |
| FA2.02 | The CP MUST make level/s of assurance for the Credential subject information available to Holders, Relying Parties and Facilitation Providers. | AUDIT3.2 – Identification Standards conformance certificate/s  AUDIT3.1b – Credential Management document (or equivalent) containing information about the method/s for declaring levels. |
| FA2.03 | The CP MUST provide mechanisms, consistent with the intended assurance levels, that enable the Credential to be recognised as bona fide. | AUDIT3.1c – Credential Management document (or equivalent) containing detailed information about the technologies and techniques used to ensure authenticity and uniqueness of the Credential. |
| FA2.04 | The CP MUST provide mechanisms, consistent with the intended assurance levels, that enable the Credential Provider to be recognised as bona fide. | AUDIT3.1d – Credential Management document (or equivalent) containing detailed information that describes technologies and techniques used to ensure the recognition and authenticity of Credential Provider. |
| ***Objective 3*** | ***Credential is privacy-preserving*** |  |
| FA3.01 | The CP MUST reduce the ability for Relying Parties to correlate holders by not including the holder’s unique Entity Information identifier as part of a Credential. | AUDIT1.4d – Privacy Impact Assessment containing information about use of the Entity Information identifier (IPP13). |
| FA3.02 | The CP MUST support minimisation of information by enabling the use of partial sets of Credential subject information, when possible. | AUDIT1.4e – Privacy Impact Assessment containing information about the disclosure of information during Credential presentation (IPP11). |
| ***Objective 4*** | ***Participation is inclusive*** |  |
| FA4.01 | The CP MUST identify the population of Entities who will require the Credential. | AUDIT1.1 – Completed Identification Risk Assessment/s  or AUDIT1.2 – Other risk assessment based on ISO31000 |
| FA4.02 | The CP MUST support any Entity within the identified population to become a Credential holder. | AUDIT3.1e – Credential Management document (or equivalent) containing a description of the application process and how it meets the population needs. |
| ***Objective 5*** | ***Credential is maintained*** |  |
| FA5.01 | The CP MUST provide the means for the Credential subject information contained in the Credential to be updated, by either:  • enabling Credential subject information in the Credential to be changed, or  • replacing the Credential, or  • establishing synchronous links to maintained sources of Credential subject information. | AUDIT3.1f – Credential Management document (or equivalent) containing details about the Credential holders’ ability to manage their Credential. |
| FA5.02 | The CP MUST provide the means for the holder to cancel a Credential. | AUDIT3.1f – Credential Management document (or equivalent) containing details about the Credential holders’ ability to manage their Credential. |
| FA5.03 | The CP MUST provide the means for the holder to report the loss or compromise of a Credential and receive support. | AUDIT3.1f – Credential Management document (or equivalent) containing details about the Credential holders’ ability to manage their Credential. |
| FA5.04 | The CP MUST provide the means for addressing holder complaints or problems arising from Credential establishment and maintenance. | AUDIT3.1g – Credential Management document (or equivalent) containing information about complaints handling. |
| FA5.05 | The CP MUST provide the means for addressing holder and Relying Party complaints or problems arising from non-facilitated Credential presentation. | AUDIT3.1g – Credential Management document (or equivalent) containing information about complaints handling. |
| FA5.06 | The CP MUST be able to update the Credential status to prevent its use, even if the responses to authentication challenges are successful, and can either:  • suspend the Credential, allowing for recovery in the future; or  • revoke, permanently disable or delete the Credential. | AUDIT3.1h – Credential Management document (or equivalent) containing Credential status management procedures. |
| FA5.07 | The CP MUST set an expiry on a Credential where the usage and risk indicates this to be appropriate. | AUDIT3.1h – Credential Management document (or equivalent) containing Credential status management procedures. |
| FA5.08 | The CP MUST log all activity within the system, including but not limited to:  • who did the action  • when the action occurred  • what the action was – create, read, update or delete  • what was changed by the action – before and after. | AUDIT3.1i – Credential Management document (or equivalent) containing information about system logging and monitoring. |
| FA5.09 | The CP MUST support additional confidence in the integrity of the Credential by taking preventative measures including but not limited to:  • auditing logs  • monitoring activities for adverse behaviours  • undertaking counter-fraud measures. | AUDIT3.1i – Credential Management document (or equivalent) containing information about system logging and monitoring. |
| FA5.10 | The CP MUST provide notifications to the holder that allow them to self-detect potential compromise, these can include but are not limited to:  • the last time the holder accessed their Credential (where applicable)  • any change made to the holder’s Credential. | AUDIT3.1h – Credential Management document (or equivalent) containing Credential status management procedures. |