**Conformance Workbook - Information and Binding Assurance**

This workbook outlines the evidence that needs to be provided to the Assessor for them to audit conformance with the Information Assurance and Binding Assurance Standards (effective 1 Oct 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 |  |  |  |
|  | AUDIT1.3 – Information Management document **(or an equivalent)** containing:   1. a rationale for the information chosen and analysis of likely duplication, 2. information about how investigations will be carried out 3. a description of the functionality of account access logs and the authenticator register, 4. information about handling unsuccessful binding attempts, 5. rationale and process for enforcing single Entity registration. |  |  |  |
|  | AUDIT1.4 – Privacy Impact Assessment containing:   1. information collected and purpose (IPP1), 2. details about information that will be retained and why (IPP5 and IPP9), 3. details about information disposal (IPP9). |  |  |  |
|  | AUDIT1.5 – List of data standards used |  |  |  |
|  | AUDIT1.6 - Levels of Assurance Document  For each piece of information, describe the processes and functionality for meeting the information and binding controls, at the assurance level being sought.  *This can be done as a table (template available) and attached to the Information Management document.* |  |  |  |
| NA | AUDIT1.7 - Discussion |  |  |  |
|  |  |  |  |  |

**Controls and the audit evidence**

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

**Information Assurance Controls**

|  |  |  |
| --- | --- | --- |
| **Reference** | **Objective/Control description** | **Audit evidence/criteria** |
| ***Objective 1*** | ***Information risk is understood*** |  |
| IA1.01 | The RP MUST carry out an assessment of the information risk posed by any service before offering it. | AUDIT1.1 – Completed Identification Risk Assessment/s  or AUDIT1.2 – Other risk assessment based on ISO31000 |
| ***Objective 2*** | ***Information is protected*** |  |
| IA2.01 | The RP MUST collect enough distinctive information, related to an entity, for it to be distinguishable from another entity’s information. | AUDIT1.3a – Information Management document (or equivalent) containing a rationale for the information chosen and analysis of likely duplication |
| IA2.02 | The RP MUST have a justifiable need for every piece of information it collects. | AUDIT1.4a – Privacy Impact Assessment containing information collected and purpose (IPP1) |
| IA2.03 | The RP MUST store only the information it requires to carry out its purpose. | AUDIT1.4b – Privacy Impact Assessment containing details about information that will be retained and why (IPP5 and IPP9) |
| IA2.04 | Where information is collected for the sole purpose of verifying required information, the RP MUST discard this information once verification is complete. | AUDIT1.4c – Privacy Impact Assessment containing details about information disposal (IPP9) |
| ***Objective 3*** | ***Information is accurate*** |  |
| IA3.01 | The RP SHOULD use recommended data format standards for the collection and storage of information. | AUDIT1.5 – List of data standards used |
| IA3.02 | The RP MUST establish the level of information assurance (IA) required, for each piece of information collected. | AUDIT1.1 – Completed Identification Risk Assessment/s  or AUDIT1.2 – Other risk assessment based on ISO31000 |
| IA3.03 | The RP verifies each piece of information using evidence at the established level of information assurance (IA). | AUDIT1.6 – Levels of Assurance Document |
| IA3.04 | The RP MUST NOT assign a level of assurance to evidence whose level has not been declared. | AUDIT1.7 – Discussion |
| ***Objective 4*** | ***Quality of evidence*** |  |
| IA4.01a | The RP establishes the quality of the credential or database evidence is consistent with the level of information assurance (IA) required. | AUDIT1.6 – Levels of Assurance Document |
| IA4.01b | The RP establishes the quality of the subject or 3rd party statement is consistent with the level of information assurance (IA) required. | AUDIT1.6 – Levels of Assurance Document |
| IA4:02a | The RP establishes if any credential or database evidence has a registered status (such as suspended or revoked), that makes it unusable. | AUDIT1.6 – Levels of Assurance Document |
| IA4:02b | The RP establishes if any subject or 3rd party statement has a contradiction, that makes it unusable. | AUDIT1.6 – Levels of Assurance Document |
| ***Objective 5*** | ***Verification integrity is maintained*** |  |
| IA5:01 | The RP applies counter fraud techniques, where possible. | AUDIT1.6 – Levels of Assurance Document |
| IA5:02 | The RP MUST store appropriate detail about the information verification and evidence to enable queries or investigation in the future. | AUDIT1.3b – Information Management document (or equivalent) containing information about how investigations will be carried out. |
|  |  |  |

**Entity Binding Assurance Controls**

|  |  |  |
| --- | --- | --- |
| **Reference** | **Objective/Control description** | **Audit evidence/criteria** |
| ***Objective 1*** | ***Binding risk is understood*** |  |
| BA1.01 | The RP MUST carry out an assessment of the binding risk posed by any service before offering it. | AUDIT1.1 – Completed Identification Risk Assessment/s  or AUDIT1.2 – Other risk assessment based on ISO31000 |
| ***Objective 2*** | ***Entity can claim an instance of Entity Information*** |  |
| BA2.01 | The RP MUST ensure the Entity provides enough information to identify a distinct instance of Entity Information. | AUDIT1.3a – Information Management document (or equivalent) containing a rationale for the information chosen and analysis of likely duplication. |
| BA2.02 | The RP MUST be able to identify when an instance of Entity Information has been claimed. | AUDIT1.3c – Information Management document (or equivalent) containing a description of the functionality of account access logs and the authenticator register. |
| ***Objective 3*** | ***Entity is the subject of Entity Information*** |  |
| BA3.01 | The RP MUST establish the level of binding assurance (BA) required, for establishing the relationship between the Entity and the information collected. | AUDIT1.1 – Completed Identification Risk Assessment/s  or AUDIT1.2 – Other risk assessment based on ISO31000 |
| BA3.02 | The RP binds each piece of Entity Information at the established level of binding assurance (BA) required, using the following binding factor types:  • knowledge factors that are not publicly known, easily determined or predictable; • possession factors that contain enough features to assess as genuine;  • biometric factors with appropriate measures to detect spoofing attempts (for example, recordings, masks, makeup or prosthetics etc.) | AUDIT1.6 – Levels of Assurance Document |
| BA3.03 | The RP MUST NOT assign a level of assurance to the binding, where an Authenticator or Credential is used, if the level has not been declared. | AUDIT1.7 – Discussion |
| BA3.04 | The RP MUST limit the number of unsuccessful attempts to bind, disallow further attempts and trigger further investigation. | AUDIT1.3d – Information Management document (or equivalent) containing information about handling unsuccessful binding attempts. |
| ***Objective 4*** | ***Entity uniqueness in a context*** |  |
| BA4.01 | The RP SHOULD ensure an Entity cannot claim more than 1 instance of Entity Information, where Entity uniqueness is required by the context. | AUDIT1.7 – Discussion  AUDIT1.3e– Information Management document (or equivalent) containing rationale and process for enforcing single Entity registration. |
| ***Objective 5*** | ***Entity Binding integrity is maintained*** |  |
| BA5.01 | The RP retests Entity Binding at least once every 5 years to ensure it remains consistent with the level of binding assurance (BA) required. | AUDIT1.6 – Levels of Assurance Document |
| BA5.02 | The RP applies counter fraud techniques, where possible. | AUDIT1.6 – Levels of Assurance Document |
| BA5.03 | The RP MUST store appropriate detail about the Entity binding process to enable queries or investigation in the future. | AUDIT1.3b – Information Management document (or equivalent) containing information about how investigations will be carried out. |
|  |  |  |