**Conformance Workbook - Authentication Assurance**

This workbook outlines the evidence that needs to be provided to the Assessor for them to audit conformance with the Authentication Assurance Standard (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 |  |  |  |
|  | AUDIT1.6 - Levels of Assurance Reference Document |  |  |  |
|  | AUDIT2.1 – Authentication Management document **(or equivalent)** containing:   1. information about the control of holder behaviour, 2. information about processes related to lost or compromised Authenticators 3. information about the Authenticator establishment process, 4. information about the Authenticator challenge response and compromise testing, 5. information about Authenticator Registration management, 6. information about how investigations will be carried out, 7. analysis of effectiveness of physical credential security features. |  |  |  |
|  | AUDIT2.2 – Authentication Factor Level Document  For each authentication factor, describe the processes and functionality for meeting the factor specific controls, at the assurance level being sought.  *This can be done in table format (template available) and attached to the Authentication Management document.* |  |  |  |
|  |  |  |  |  |

**Controls and the audit evidence**

The following tables list the controls and the Audit evidence applicable to each. Where level apply this is indicated.

**Authentication Assurance Controls**

|  |  |  |
| --- | --- | --- |
| **Reference** | **Objective/Control description** | **Audit evidence/criteria** |
| ***Objective 1*** | ***Authentication risk is understood*** |  |
| AA1.01 | The RP MUST carry out an assessment of the authentication 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*** | ***Ensure correct authenticator holder behaviour*** |  |
| AA2.01 | The RP MUST issue terms and conditions describing the Authenticator holder’s obligations, including: • the Authenticator is for the sole use of the Authenticator holder • explaining how the holder will keep the Authenticator safe • that the holder reports loss of the Authenticator including unauthorised use, sharing, theft of the Authenticator, possible compromise, or any other suspected loss of control of the Authenticator | AUDIT2.1a – Authentication Management document (or equivalent) containing information about the control of holder behaviour. |
| AA2.02 | The RP MUST provide communication to Authenticator holders reminding them about their obligations, including:  • the Authenticator is for the sole use of the holder • the holder will keep the Authenticator safe • that the holder reports loss of the Authenticator including unauthorised use, sharing, theft of the Authenticator, possible compromise, or any other suspected loss of control of the Authenticator | AUDIT2.1a – Authentication Management document (or equivalent) containing information about the control of holder behaviour. |
| AA2.03 | The RP limits the ability to share an Authenticator by implementing 2 different factor types. | AUDIT2.1a – Authentication Management document (or equivalent) containing information about the control of holder behaviour.  AUDIT2.2 – Authentication Factor Control Level Reference document |
| AA2.04 | The RP allows no more than 30 consecutive unsuccessful attempts to authenticate by any factor, disables the account and triggers further investigation. | AUDIT2.1a – Authentication Management document (or equivalent) containing information about the control of holder behaviour.  AUDIT2.2 – Authentication Factor Control Level Reference document |
| AA2.05 | The RP MUST provide the means for the holder to report loss or compromise of an Authenticator, and can either: • deregister the Authenticator and support a process for reregistration; or • if appropriate, close the associated account and require reenrolment | AUDIT2.1b – Authentication Management document (or equivalent) containing information about processes related to lost or compromised Authenticators. |
| ***Objective 3*** | ***Entity binding and Authenticator strength are consistent*** |  |
| AA3.01 | The RP MUST ensure that the Entity Binding is done in the same transaction session as Authenticator is established. | AUDIT2.1c – Authentication Management document (or equivalent) containing information about the Authenticator establishment process. |
| AA3.02 | The RP MUST ensure the strength of the Authenticator is consistent with the level of binding assurance (BA) required. | AUDIT1.6 - Levels of Assurance Document  AUDIT2.1c – Authentication Management document (or equivalent) containing information about the Authenticator establishment process. |
| ***Objective 4*** | ***Entity can control Authenticator*** |  |
| AA4.01 | The RP MUST ensure that the Entity can respond to all the Authenticator’s challenges before the Authenticator is recorded as active in Entity Information. | AUDIT2.1d – Authentication Management document (or equivalent) containing information about the Authenticator challenge response and compromise testing. |
| AA4.02 | The RP establishes if the Authenticator has been previously compromised to the extent it makes it unusable. | AUDIT2.1d – Authentication Management document (or equivalent) containing information about the Authenticator challenge response and compromise testing.  AUDIT2.2 – Authentication Factor Level Document |
|  |  |  |
| ***Objective 5*** | ***Authenticator registration status is maintained*** |  |
| AA5.01 | The RP MUST record enough information in Entity Information for an Authenticator to be recognised and its Authenticator Registration status to be managed. | AUDIT2.1c – Authentication Management document (or equivalent) containing information about the Authenticator establishment process.  AUDIT2.1e – Authentication Management document (or equivalent) containing information about Authenticator Registration management. |
| AA5.02 | The RP MUST be able to update the Authenticator Registration status to prevent authentication occurring, even if the responses to challenges are successful. | AUDIT2.1e – Authentication Management document (or equivalent) containing information about Authenticator Registration management. |
| AA5.03 | The RP MUST NOT accept an authentication event as successful unless the Authenticator Registration status allows. | AUDIT2.1c – Authentication Management document (or equivalent) containing information about the Authenticator establishment process. |
| AA5.04 | The RP MUST be able to set an expiry on an Authenticator Registration where the implementation indicates this to be desirable. | AUDIT2.1c – Authentication Management document (or equivalent) containing information about the Authenticator establishment process. |
| ***Objective 6*** | ***Authentication events can be investigated*** |  |
| AA6.01 | The RP MUST record appropriate detail about the Authenticator establishment process to enable queries or investigation in the future. | AUDIT2.1f – Authentication Management document (or equivalent) containing information about how investigations will be carried out. |
| AA6.02 | The RP MUST store appropriate detail about an authentication event to enable queries or investigation in the future. | AUDIT2.1f – Authentication Management document (or equivalent) containing information about how investigations will be carried out. |
| ***Factor specific controls*** | | |
| ***Objective 7*** | ***Protect a knowledge factor response from being guessed or discovered*** |  |
| AA7.01 | The RP implements minimum levels of complexity on any knowledge factor response (secret). | AUDIT2.2 – Authentication Factor Level Document |
| AA7.02 | The RP limits the creation of easily guessable knowledge factor responses by disallowing repetition or patterns and where the authenticator has the form of an online password, apply the following exclusions (as applicable to the character sets being used): • disallow repetitive or sequential characters • disallow specific words, for example the identifier (e.g. username), name of the service etc. • disallow singular dictionary words and common character substitutions • disallow passwords contained in blacklists (usually include overly common combinations and compromised passwords) | AUDIT2.2 – Authentication Factor Level Document |
| AA7.03 | The RP implements maximum limits for unsuccessful attempts and prevents further attempts for a minimum period. | AUDIT2.2 – Authentication Factor Level Document |
| AA7.04 | The RP prevents use of a guessed or discovered knowledge factor by combining it with an authentication factor of another type. | AUDIT2.2 – Authentication Factor Level Document |
| ***Objective 8*** | ***Prevent use of a physically acquired possession factor*** |  |
| AA8.01 | The RP prevents use of a physically acquired possession factor by combining it with an authentication factor of another type. | AUDIT2.2 – Authentication Factor Level Document |
| ***Objective 9*** | ***Protecting against replication, forgery, or spoofing of possession and biometric factors*** |  |
| AA9.01 | The RP MUST protect against replication or forgery of a physically presented authenticator by incorporating features that ensure the cost of doing so is relative to the level of assurance. | AUDIT2.1g – Authentication Management document (or equivalent) containing analysis of effectiveness of physical credential security features. |
| AA9.02 | The RP uses dynamic, non-predictable responses to non-physical challenges on possession factors and limits the response validity to a maximum of 10 minutes or 1 minute, where little messaging delay exists. | AUDIT2.2 – Authentication Factor Level Document |
| AA9.03 | The RP MUST, for responses to non-physical challenges on possession factors, utilise a minimum complexity of:  • 6 numeric characters; or • 4 alphanumeric characters; or  • an equivalent level for other codes such as pictograms | AUDIT2.2 – Authentication Factor Level Document |
| AA9.04 | The RP addresses spoofing of biometric challenges by ensuring the biometric response is obtained from the person using appropriate measures to detect spoofing attempts (e.g. recordings, masks, makeup or prosthetics etc.). | AUDIT2.2 – Authentication Factor Level Document |
| AA9.05 | The RP obtains biometric factor samples in person or remotely incorporating liveness checking which demonstrates at least 90% resistance to presentation attacks. | AUDIT2.2 – Authentication Factor Level Document |
| ***Objective 10*** | ***Managing biometric factor probability*** |  |
| AA10.01 | The RP reduces the occurrence of false positives in biometric comparisons by using:  • manual comparison of the biometric characteristic by a trained operator • systematic comparison with a rate of <0.01% false positives, based on a one-to-one comparison | AUDIT2.2 – Authentication Factor Level Document |
| AA10.02 | The RP protects against the probabilistic nature of biometric comparisons by combining it with an authentication factor of another type. | AUDIT2.2 – Authentication Factor Level Document |
|  |  |  |