|  |
| --- |
| Documenting your ISMS self-assessment - Remove before use  Category 2A providers may self-assess their ISMS against the ISO27001 standard. The department requires the self-assessment to address the following content requirements:   1. The provider has assessed the ISMS conformance with each of the requirements within ISO27001 clauses 4-10 and identified any remaining issues. 2. The provider has asserted that the status of their ISMS is accurately described in the Statement of Applicability (SoA), in that:    1. All ISM OFFICIAL and OFFICIAL: Sensitive controls have been considered for inclusion.    2. All controls determined as not applicable include an appropriate justification.    3. All controls determined as applicable include a description of, and a reference to the filename of the provider’s policies, procedures, or other documentation that achieve the intent of the control within the ISMS.    4. The implementation status of applicable controls is accurately recorded in the SoA. 3. The provider has included an action plan and expected timeframes to address remaining gaps, and to implement any applicable but currently unimplemented controls.   This template is to be used as the basis of your ISO27001 management clauses self-assessment, and submitted together with your Scope document and SoA. |
| Examples used are not definitive or exhaustive. Other information may be relevant to your circumstances. |

**Declaration**

[To be completed by a Director and/or Company Secretary, or business owner as required by the Corporations Law as relevant to the provider’s incorporation]

[We/I] the undersigned declare to the best of [our/my] knowledge and belief that the information contained in this report is complete and accurate as at the date of issue. With the exception of information described in this report under the heading “known issues”, all controls described in this report and the attached Statement of Applicability are in place and are expected to operate effectively into the foreseeable future.

[We/I] further declare that [we are/I am] aware of all conformance issues described in this report and shall ensure that persons with organisational governance responsibility monitor actions to address each gap until complete.

[Delete if this report is not an annual “accreditation maintenance” report: We have disclosed to the department, in relation to the period since our previous self-assessment report of [date]:

1. All known instances of non-compliance or suspected non-compliance with laws and regulations, fraud or suspected fraud, and uncorrected deviations in controls attributable to [Provider] that may affect the department or any individuals that [Provider] holds record of as a result of the deed(s).

2. All control deficiencies of which we are aware

3. All instances, of which we are aware, where controls have not operated as described]

**[Sole trader:** Signed by [name] in the presence of:

Signature of witness Signature of signatory

Name of witness (print) Name of signatory (print)

**/Partnership:** Signed for and on behalf of [partnership name] in the presence of:

Signature of witness Signature of partner

Name of witness (print) Name of partner (print)

**/Company:** Signed on behalf of {company name] in accordance with s.127 of the Corporations Act 2001 (Cth) by:

Signature of Director Signature of Director/Secretary

Name of Director (print) Name of Director/Secretary (print)

**/Company with single Director:** Signed on behalf of [company name] in accordance with s.127 of the Corporations Act 2001 (Cth.) by:

Signature of Sole Director/Secretary who states they are the sole director and sole secretary

Name of Sole Director/Secretary (print) ]

**Typical ISMS Self-assessment report headings**

# Executive Summary

[Consider the purpose of the self-assessment, how was it conducted, who conducted it, and what were the findings/conclusions?]

[Summarise the overall status of the ISMS and list any areas of non-conformance with the ISO27001 standard.]

[Summarise the required actions and expected timeframes to fully implement the ISMS described by the SoA. Include a specific reference to the SoA by version/date and name.]

# Conformance with ISO 27001 requirements

## Context of the Organisation

### Cl. 4.1: Understanding the organisation and its context

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the ISO 27001 standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 4.2: Understanding the needs and expectations of interested parties

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 4.3: Determining the scope of the ISMS

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 4.4: ISMS

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

## Leadership

### Cl. 5.1: Leadership and commitment

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 5.2: Policy

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 5.3: Organisational roles, responsibilities and authorities

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

## Planning

### Cl. 6.1: Actions to address risks and opportunities

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

[Include in this section statements to assert that, consistent with Cl. 6.1.3:

* the ISMS described by the SoA (include a specific reference to the SoA by version/date and name) has considered all ISO 27001 Annex A controls as well as controls relevant to protecting OFFICIAL information sourced from the (month, year) release of ISM.
* controls determined to be not applicable have been appropriately justified with comments in the SoA.
* controls determined to be applicable have been referenced to ISMS documentation or other evidence of inclusion in the ISMS as appropriate.]

### Cl. 6.2: Information security objectives and planning to achieve them

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

## Support

### Cl. 7.1: Resources

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 7.2: Competence

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 7.3: Awareness

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 7.4: Communication

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 7.5: Documented information

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

## Operation

### Cl. 8.1: Operational planning and control

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 8.2: Information security risk assessment

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 8.3: Information security risk treatment

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

## **Performance evalua**tion

### Cl. 9.1: Monitoring, measurement, analysis and evaluation

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 9.2: Internal audit

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 9.3: Management review

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

## Improvement

### Cl. 10.1: Nonconformity and corrective action

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

### Cl. 10.2 Continual improvement

|  |  |
| --- | --- |
| Requirement: | Xxxxxxx (obtain details from the standard) |
| Description: | High level description of how the ISMS conforms with the requirement, include references to documented evidence where possible |
| Assessment: | (Fully conforms / partially conforms / does not conform) |
| Details of non-conformance | For partial conformance or non-conformance only – describe the issue |
| Action required to achieve full conformance | For partial conformance or non-conformance only – describe actions required to fully conform with the requirement |
| Expected completion date | For partial conformance or non-conformance only – list the month/year when actions are expected to be complete |

# Status of applicable controls identified in the SoA

[State that the implementation status of applicable controls has been accurately documented in the SoA (include a specific reference to the SoA by version/date and name).]

[Summarise the applicable controls that are not yet fully implemented, and the required actions and expected timeframes before these controls will be in place.]   
OR  
[Record this information in additional columns in the SoA, and refer readers to it (for example: “Some applicable controls are not fully implemented at the date of this self-assessment report. Details are reflected in the “implementation status” (amend as appropriate) column of the SoA. For each applicable but unimplemented control included in the SoA, information describing actions and expected timeframes to implement these controls is included in columns (X) and (Y) of the SoA.”]

[Conclude by stating that “(Provider)’s performance evaluation and improvement controls are being applied to track the status of these controls until they are in place.”]

# Known issues

At the date of this report, [Provider] is aware of the following issues:

1. [Only relevant if there are known instances of non-compliance or suspected non-compliance with laws and regulations, fraud or suspected fraud, or uncorrected deviations in controls] Over the past twelve months [Provider] has experienced instances of non-compliance (or suspected non-compliance) with laws and regulations; and/or instances of fraud (or suspected fraud). These events may affect the department and/or any individuals that [Provider] holds record of as a result of the deed(s). These have included:
   1. [Details of legislative noncompliance events and fraud events
   2. …]

[Provider] has taken all necessary steps to remedy these instances and has reported them to the department and relevant authorities.

1. [Only relevant if there have been significant changes to the Provider’s business and therefore the scope of the ISMS] Over the past twelve months the following events have occurred which impacted on the scope of our business and services within the scope of the accredited Information Security Management System.
   1. Details of new or changed Deeds with the department
   2. Details of corporate restructuring/rebranding/mergers and acquisitions
   3. Details of new or changed physical locations associated with program-related services
   4. Details of new or changed ICT systems including TPES use
   5. Details of significantly changed security roles/responsibilities
   6. Details of new or changed third parties (subcontractors, managed service providers, other service providers relevant to information security)

[Provider] has considered security risks associated with these events and has updated the accredited ISMS’ key artefacts to account for relevant changes, including the ISMS Scope and Statement of Applicability. The changes to the ISMS scope have been included in relevant internal audits and in management’s review of the ISMS that has informed this self-assessment report. [If significant changes such as the above have occurred in the past year please include a copy of your revised ISMS Scope document, reflecting these changes, alongside your annual self-assessment report and SoA].

1. [Only relevant if some controls have not yet been implemented] As disclosed in section three of this self-assessent report and described in the attached SoA, certain planned control measures identified in the attached SoA, [insert unique filename here], are not yet fully in place. These are identified in the SoA as any control where the “implementation status” column has a value of “1 - Planned but not implemented” or “2 - Partially implemented, full benefit cannot be expected”.   
     
   [Provider] has documented and resourced firm plans to complete the implementation of these controls in the timeframes indicated in the attached Statement of Applicability.
2. [Only relevant if the Provider is aware that some security controls have not performed as intended] Some of our implemented security controls have not functioned as intended over the past twelve months. This includes:
3. [List any known instances of a control measure not working properly
4. ….]

Actions to address these issues have been identified, including:

* 1. [List actions already completed; and any actions not yet completed together with their expected completion dates
  2. ...]

[Provider] has implemented effective oversight and monitoring mechanisms to track progress of these actions until their completion.

Include in this section details of any other issues that should be disclosed to the department.