# Remove this page before submission

|  |
| --- |
| GuidanceCategory 2A providers will self-assess their ISMS against the ISO/IEC 27001:2013 standard. The department requires the self-assessment to address the following requirements:1. The provider has assessed the ISMS conformance with each of the requirements within ISO/IEC 27001:2013 clauses 4-10 and identified any remaining gaps.
2. The provider has included an action plan and expected timeframes to address the remaining gaps.
3. The provider has asserted that the status of their ISMS is accurately described in the Statement of Applicability (SoA), in which:
	1. All OFFICIAL: Sensitive ISM controls have been considered for inclusion.
	2. All controls determined as not applicable include an appropriate justification.
	3. All controls determined as applicable include implementation details, 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.
	5. The implementation plan for each control not yet fully implemented is recorded.
4. The provider has reported known issues and change of circumstances.

This template is to be used as the basis of your ISO/IEC 27001:2013 management clauses self-assessment and submitted together with your Scope document and SoA. |

# Remove this page before submission

# Declaration

I, the undersigned, am duly authorised by the organisation named below to make this declaration, and confirm on behalf of the organisation, that to the best of my knowledge the information contained in this Self-Assessment Report is complete and accurate as at the date of signature.

I declare that I am aware of all conformance issues (if any) as described in the Section 2 of this Self-Assessment Report and shall ensure that persons with organisational governance responsibility monitor actions to address each instance of non-conformance until resolved.

I further declare that the status of control implementations for our Information Security Management System (ISMS) is accurately described in the Statement of Applicability (SoA) attached separately to this Self-Assessment Report. I will ensure that evidence of control implementation is available should the department request it.

I have disclosed in Section 4 of this Self-Assessment Report:

* All known instances (if any) of non-compliance or suspected non-compliance with relevant laws and regulations, fraud or suspected fraud, and uncorrected deviations in controls attributable to the organisation that may affect the department or any individuals that the organisation holds record of.
* All change of circumstances (if any) that has impacted or may have impacted the scope of the ISMS and the risk profile.

|  |  |
| --- | --- |
| Organisation’s legal name |  |
| ABN/ACN |  |
| Legal Address |  |
| Authorised representative name |  |
| Authorised representative position |  |
| Signature |  |
| Date |  |

# RFFR Self-Assessment Report

## Summary of conformance status

|  |  |  |
| --- | --- | --- |
| Clauses | Titles | Status |
| 4 | **Context of the organization** |  |
| 4.1 | Understanding the organization and its context | Choose an item. |
| 4.2 | Understanding the needs and expectations of interested parties | Choose an item. |
| 4.3 | Determining the scope of the information security management system | Choose an item. |
| 4.4 | Information security management system | Choose an item. |
| 5 | **Leadership** |  |
| 5.1 | Leadership and commitment | Choose an item. |
| 5.2 | Policy | Choose an item. |
| 5.3 | Organizational roles, responsibilities and authorities | Choose an item. |
| 6 | **Planning** |  |
| 6.1 | Actions to address risks and opportunities | Choose an item. |
| 6.2 | Information security objectives and planning to achieve them | Choose an item. |
| 7 | **Support** |  |
| 7.1 | Resources | Choose an item. |
| 7.2 | Competence | Choose an item. |
| 7.3 | Awareness | Choose an item. |
| 7.4 | Communication | Choose an item. |
| 7.5 | Documented information | Choose an item. |
| 8 | **Operation** |  |
| 8.1 | Operational planning and control | Choose an item. |
| 8.2 | Information security risk assessment | Choose an item. |
| 8.3 | Information security risk treatment | Choose an item. |
| 9 | **Performance evaluation** |  |
| 9.1 | Monitoring, measurement, analysis and evaluation | Choose an item. |
| 9.2 | Internal audit | Choose an item. |
| 9.3 | Management review | Choose an item. |
| 10 | **Improvement** |  |
| 10.1 | Nonconformity and corrective action | Choose an item. |
| 10.2 | Continual improvement | Choose an item. |

## Conformance with ISO/IEC 27001:2013 requirements

### Clause 4 – Context of the organization

#### 4.1: Understanding the organization and its context

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

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

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 4.3: Determining the scope of the information security management system

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 4.4: Information security management system

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

### Clause 5 - Leadership

#### 5.1: Leadership and commitment

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 5.2: Policy

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 5.3: Organizational roles, responsibilities and authorities

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

### Clause 6 - Planning

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

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

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

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

### Clause 7 - Support

#### 7.1: Resources

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 7.2: Competence

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 7.3: Awareness

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 7.4: Communication

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 7.5: Documented information

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

### Clause 8 - Operation

#### 8.1: Operational planning and control

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 8.2: Information security risk assessment

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 8.3: Information security risk treatment

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

### Clause 9 - Performance evaluation

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

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 9.2: Internal audit

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 9.3: Management review

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

### Clause 10 - Improvement

#### 10.1 Nonconformity and corrective action

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

#### 10.2 Continual improvement

|  |  |
| --- | --- |
| Requirements | [Obtain and copy details from the ISO/IEC 27001:2013 standard] |
| Self-assessment | Choose an item. |
| Implementation details | [Provide a summary of how the organisation conforms with the requirements of this sub-clause, including references to documented evidence where possible] |
| Identified gaps |  |
| Actions required to achieve full conformance |  |
| Expected completion date |  |

## Control implementations

As a result of our self-assessment at the organisation, the status of control implementations for our Information Security Management System (ISMS) is accurately described in the provided Statement of Applicability (SoA), in which:

* All OFFICIAL: Sensitive ISM controls have been considered for inclusion.
* All controls determined as not applicable include an appropriate justification.
* All controls determined as applicable include implementation details, and a reference to the organisation’s policies, procedures, or other documentation that support the control objectives.
* The implementation plan for each control not yet fully implemented is recorded and monitored.

## Known issues and changes

Over the past twelve months, the organisation Choose an item. experienced instances of non-compliance (or suspected non-compliance) with laws and regulations, and/or instances of fraud (or suspected fraud), which may affect the department and/or any individuals that our organisation holds record of.

[list the instances of non-compliance if applicable]

Over the past twelve months, the organisation Choose an item. had change of circumstances that has impacted or may have impacted the ISMS scope and the risk profile.

[list the change of circumstances if applicable]

The organisation has considered security risks associated with these events and has updated key artefacts to account for relevant changes, including the ISMS Scope and SoA which has informed this Self-Assessment Report.