**Information Security Management System (ISMS)**

**ASSURANCE AUDIT REPORT**

**<agency name>**

**< month year>**

Document Security Classification: < OFFICIAL / SENSITIVE / PROTECTED >

Document Control Sheet

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Key changes made | Author/s | Reviewer/s |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Copyright information**

For internal Queensland Government use only. © The State of Queensland 2025

**Attribution**

The copyright material created by the State of Queensland in this document may be copied on condition that the State is acknowledged as the owner.

**Contact us**

Enquiries about copyright and use of material in this document can be directed to [cybersecurityunit@qld.gov.au](mailto:cybersecurityunit@qld.gov.au)

**Contents**

[1. Introduction 4](#_Toc40711728)

[1.1. Background 4](#_Toc40711729)

[1.2. Objective 4](#_Toc40711730)

[1.3. Criteria 4](#_Toc40711731)

[1.4. Scope 4](#_Toc40711732)

[1.5. Approach 4](#_Toc40711733)

[1.6. Detailed Audit Approach and Timelines 5](#_Toc40711734)

[1.7. Definitions 5](#_Toc40711735)

[1.8. Assumptions 6](#_Toc40711736)

[1.9. Acknowledgements 6](#_Toc40711737)

[1.10. Audit Completed by 6](#_Toc40711738)

[2. Executive Summary 7](#_Toc40711739)

[2.1. Findings overview – positive audit findings 7](#_Toc40711740)

[2.2. Findings overview – majNC, minNC, AOC and OFI 8](#_Toc40711741)

[2.2.1. Previous outstanding audit findings 9](#_Toc40711742)

[3. Results overview 10](#_Toc40711743)

[3.1. General Controls summary 10](#_Toc40711746)

[3.2. Annex A Clauses summary 11](#_Toc40711747)

[3.3. Conclusion 12](#_Toc40711748)

[3.4. Management Acceptance 12](#_Toc40711749)

# Introduction

# Background

The [Information and cyber security policy (IS18)](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-security-policy-is18-2018) mandates that agencies implement an ISMS based on the current version of ISO 27001 and obtain appropriate information security assurance.

This Assurance Audit is seeking to fulfil the requirement Queensland Government Departments and Agencies have in accordance with IS18, [policy requirement 1](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-security-policy-is18-2018).

# Objective

The objective of the assurance review is to assess the maturity of the agency’s ISMS implementation and effectiveness of operation of an ISMS against the ISO 27001: 2013.

# Criteria

The ISMS is assessed against the requirements of the ISO/IEC 27001:2013 standard, the requirements of the Queensland Government Enterprise Architecture (QGEA) [Information and cyber security policy (IS18)](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-security-policy-is18-2018).

# Scope

The scope of the audit is closely linked with the [IS18: policy requirement 1](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-security-policy-is18-2018), and the [policy requirement 4](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-security-policy-is18-2018) stating that Accountable officers (CEO/Director-General or equivalent) must obtain security assurance to establish an understanding of information security protections and adherence to this policy.

As stated in the [Information security assurance and classification guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-security-assurance-and-classification-guideline):

* Security assurance provides accountable officers with a level of confidence that identified risks to information assets are being managed appropriately.
* The level of assurance and the resources spent of achieving the level, should be equal with the associated BIL for the information asset.
* The department’s accountable officer, advised by the executive leadership, should identify what levels of assurance are required of the department for different levels of information criticality in a departmental policy. An [example policy](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-security-assurance-and-classification-guideline#Example) is provided within the guideline to assist the agencies.

# Approach

This audit is conducted as part of the agency’s audit plan <insert the agency reference to the ISMS audit plan>

Following is the approach this audit has chosen: <choose one, delete the other>

* This audit was conducted utilising the Queensland Government interagency ISMS Assurance Audit team
* This audit was outsourced to an independent certified third party supplier: <insert supplier name>

The audit uses a standardised approach and in general follows these steps:

1. Scoping and pre-audit survey
2. Planning and preparation
3. Fieldwork
4. Analysis
5. Reporting

All audit findings are recorded in the ISMS Assurance Audit – Detailed Findings document and are summarised in this document.

# Detailed Audit Approach and Timelines

Following is a detailed Audit approach and timelines:

| Audit phase | Details of engagements, timelines, required participants etc. |
| --- | --- |
| Scoping and pre-audit survey |  |
| Planning and preparation |  |
| Fieldwork |  |
| Analysis |  |
| Reporting |  |

# Definitions

The following definitions are provided with respect to the categorisation of assurance review findings.

| Item | Description | Action Required |
| --- | --- | --- |
| Non-Conformity(majNC – MajorminNC – Minor) | An area of the management system that does not conform with the requirements of the standard. | The client is required to investigate the non-conformity and complete corrective or preventive action within the management system prior to certification being achieved or retained. |
| Area of Concern(AOC) | Relates to a single identified lapse, which would not indicate a breakdown in the control’s ability to effectively manage the processes for which it was intended. May lead to a non-conformity if not addressed. | The client is required to investigate the potential or actual non-conformity and complete corrective or preventive action within the management system. |
| Opportunity for Improvement(OFI) | An area of the system where a situation is not directly causing a non-conformity, but a change may improve the operation of the management system. | The client should review the situation and assess whether the development and implementation of a solution will add value to operations and the management system. The change should be tracked through the procedure for making improvements and preventive and corrective actions. |

# Assumptions

The following assumptions have been made prior to commencement of the audit:

1. Assumption
2. Assumption
3. Assumption

# Acknowledgements

The audit team wishes to acknowledge…

# Audit Completed by

| Name(s) | Position | Organisation | Contact details | Statement of auditor’s competence |
| --- | --- | --- |
|  |  | e.g. length of experience in ISMS audit, relevant training/education completed |

# Executive Summary

# Findings overview – positive audit findings

The following is a high level summary of positive findings the Audit team has observed:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **majNC** |  | **minNC** |  | **AOC** |  | **OFI** |
| **##** | **##** | **##** | **##** |

# Findings overview – majNC, minNC, AOC and OFI

The following is a high-level summary of Major Non-Conformances (majNC), Minor Non-Conformances (minNC)s, Area of Concern (AOC)s and Opportunity for Improvement (OFI)s, that were noted during the assurance review. Please refer the Results overview section below and Detailed Assurance Findings document for further details.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Mandatory Clauses** | Total number of observations | | | |
|  |  | majNC | minNC | AOC | OFI |
| 4 | Context of the organisation | # | # | # | # |
| 5 | Leadership |  |  |  |  |
| 6 | Planning |  |  |  |  |
| 7 | Support |  |  |  |  |
| 8 | Operation |  |  |  |  |
| 9 | Performance evaluation |  |  |  |  |
| 10 | Improvement |  |  |  |  |

The following reflects the evaluation results against the ISO/IEC 27001:2013 mandatory clauses:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Annex-A Controls** | Total number of observations | | | |
|  |  | majNC | minNC | AOC | OFI |
| A.5 | Information Security Policies | # | # | # | # |
| A.6 | Organisation of information security |  |  |  |  |
| A.7 | Human resource security |  |  |  |  |
| A.8 | Asset management |  |  |  |  |
| A.9 | Access control |  |  |  |  |
| A.10 | Cryptography |  |  |  |  |
| A.11 | Physical and environmental security |  |  |  |  |
| A.12 | Operation security |  |  |  |  |
| A.13 | Communications security |  |  |  |  |
| A.14 | System acquisition, development and maintenance |  |  |  |  |
| A.15 | Supplier relationships |  |  |  |  |
| A.16 | Information security incident management |  |  |  |  |
| A.17 | Information security aspects of business continuity management |  |  |  |  |
| A.18 | Compliance |  |  |  |  |

The following reflects the evaluation results against the Annex-A controls included in the ISO/IEC 27001: 2013 standard:

# Previous outstanding audit findings[[1]](#footnote-2)

The following is the list of open majNC and minNC from the previous ISMS assurance audit:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rating | Clause or Annex A Control ID | Issue ID | Issue description | Action Officer | Due Date |
| **majNC** | **#** or **#.#** | **YYYY-##** |  | Name Surname | DD/MM/YYYY |
| **minNC** | **#** or **#.#** | **YYYY-##** |  | Name Surname | DD/MM/YYYY |

# Results overview



# Clauses 4-10 summary

Please note the findings related to mandatory Clauses are summarised at control level (4 – 10) in order to ensure a standardised approach in terms of audit findings across Queensland Government.

Following are findings related to Clauses 4-10 grouped by rating:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rating | Issue ID | Control ID (4 - 10) | Issue description | Action Officer | Due Date |
| **majNC** | **2020-01** | **#** | Brief description of the finding. | Name Surname | DD/MM/YYYY |
|  |  |  |  |  |  |
| **minNC** | **YYYY-##** | **#** | Brief description of the finding. | Name Surname | DD/MM/YYYY |
|  |  |  |  |  |  |
| **AOC** | **YYYY-##** | **#** | Brief description of the finding. | Name Surname | DD/MM/YYYY |
|  |  |  |  |  |  |
| **OFI** | **YYYY-##** | **#** | Brief description of the finding. | Name Surname | DD/MM/YYYY |

# Annex A Controls summary

The Annex A controls are reported and summarised at sub-control level to ensure a standardised approach in terms of audit findings across Queensland Government.

For example, the Annex A control A.6 contains sub-levels A.6.1 and A.6.2 so the audit finding should be summarised at that sub-control level (A.6.1 and A.6.2) even if the sub control contains additional level of sub-controls (e.g. A.6.1.1 through to A.6.1.5).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rating | Issue ID | Annex A Control ID | Issue description | Action Officer | Due Date |
| **majNC** | **YYYY-##** | **#.#** | Brief description of the finding. | Name Surname | DD/MM/YYYY |
|  |  |  |  |  |  |
| **minNC** | **YYYY-##** | **#.#** | Brief description of the finding. | Name Surname | DD/MM/YYYY |
|  |  |  |  |  |  |
| **AOC** | **YYYY-##** | **#.#** | Brief description of the finding. | Name Surname | DD/MM/YYYY |
|  |  |  |  |  |  |
| **OFI** | **YYYY-##** | **#.#** | Brief description of the finding. | Name Surname | DD/MM/YYYY |

# Conclusion

# Management Acceptance

The actions resulting from this audit have been accepted by the agency’s ISMS executive officer:

|  |  |  |
| --- | --- | --- |
| Name | Role/Title | Signature and date |
|  |  |  |

1. If this is agency’s first ISMS audit, please indicate accordingly and delete the rest of the text under 2.2.1 including this footnote. [↑](#footnote-ref-2)