

Information Security Audit and Compliance Policy

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Statement	3
4. Roles and Responsibilities	4
5. Information Security Compliance	5
6. Information Security Auditing.....	5
6.1. Information Security Audit Programme	5
6.2. Internal Audits	6
6.2.1. Criteria for Appointment of the Internal Auditors	6
6.2.2. Methodology for Internal Audits	6
6.3. External Audits	7
7. Nonconformities and Opportunities for Improvement.....	8
8. Metrics and Reporting	9
9. Policy Review Date	9
10. Appendix A – Audit Definitions	10
11. Document Control	11
11.1. Document Revision History	11

1. Purpose

- 1.1. The purpose of this policy is to specify and communicate the requirements for conducting information security audits at the OCA and ensuring compliance with the relevant legislative, statutory, regulatory and contractual requirements.

2. Scope

- 2.1. This policy applies to all the OCA employees, contractors, consultants, suppliers and other interested third parties that have access to the OCA's information.

3. Policy Statement

- 3.1. The OCA's policy regarding information security audit and compliance is as follows:

- The OCA shall be subject to regular audits to monitor its compliance with contractual obligations and with relevant standards and regulations related with information security.
- In addition to assessing compliance, audits shall also assess the efficiency of processes and controls and identify opportunities for their improvement.
- Audits shall be objective, impartial and performed by appropriately qualified independent third parties.
- There shall be a documented information security audit programme, established and approved on an annual basis, that ensures that all relevant areas are audited in a timely fashion and in alignment with the schedule and scope of external audits required for compliance or certification against relevant standards or regulations, or mandated by any other reason.
- Any nonconformities and opportunities for improvement, whether identified through audits or by other ways, shall be recorded in a centralised register, with remediation actions to address them established with the relevant business areas, assigned ownership and tracked to completion within appropriate agreed timelines.
- The outcomes of information security audits and the status of remediation actions shall be reported in a timely fashion to and reviewed by the Finance, Employment, Audit and Risk (FEAR) Committee.

4. Roles and Responsibilities

- The IT Manager is responsible for this policy and shall ensure that this policy is up-to-date and relevant. The IT Manager is also responsible for:
 - Maintaining an up-to-date list of all legislative, statutory, regulatory and contractual requirements relevant for the OCAs information security environment;
 - Planning, establishing, implementing and maintaining an information security audit programme;
 - Reviewing and signing off correction action plans to address nonconformities;
 - Reporting to the FEAR Committee:
 - The outcomes of information security audits;
 - Relevant information security audit and compliance monitoring metrics.
 - Supporting information security audits in line with this policy, liaising with other internal teams and departments for the arrangement of interviews with and provision of documentary evidence to the auditor(s);
 - Supporting the IT Team and the heads of audited functions in the identification of corrective action plans to address the findings of audits.
- The IT Team is responsible for:
 - Supporting the IT Manager in:
 - The development of the information security audit programme;
 - The creation and maintenance of a register of information security nonconformities and opportunities of improvement;
 - Establishing corrective action plans to address nonconformities and opportunities for improvement, in liaison with the heads of the audited functions;
 - Tracking the implementation of corrective actions to completion, in liaison with the designated action owners.
- The FEAR Committee is responsible for:
 - Management overview of information security audit and compliance, including the regular review of relevant reports and metrics;
 - Approval of the information security audit programme, on an annual basis.
- The heads of audited functions are responsible for:
 - Ensuring that the required information and documentary evidence within their areas of responsibility are provided to auditors when audits are conducted;
 - Establishing corrective action plans to address nonconformities and opportunities for improvement, in liaison with the IT Manager.

- All OCA employees, contractors, consultants, suppliers and other interested third parties that have access to the OCA's information shall comply with this policy, including:
 - Reporting to the IT Manager any perceived nonconformities or opportunities for improvement related with information security policies, processes or controls;
 - Providing, where required, information and documentary evidence within their areas of responsibility to auditors when audits are conducted;
 - Implementing corrective actions assigned to them (or contributing to that implementation as required).

5. Information Security Compliance

5.1. Compliance shall be enforced with:

- Standards / frameworks that the OCA is certified against or aligned to, including ISO 27001:2022 – see the [Information Security Management System \(ISMS\) Policy](#);
- Any relevant contracts that have an information security context.
- Any relevant legal and regulatory information security requirements.

5.2. The IT Manager shall maintain, where appropriate, an up-to-date list of all legislative, statutory, regulatory and contractual requirements relevant for the OCA and its information systems, and the approach to meet these requirements.

5.3. Compliance shall be monitored and enforced through information security audits and management of identified nonconformities and opportunities for improvement, in line with sections 6 and 7 below.

6. Information Security Auditing

6.1. Information Security Audit Programme

6.1.1. The IT Manager shall plan, document, implement and maintain an information security audit programme. This programme shall:

- Take in consideration the schedule and scope of audits required for compliance or certification against relevant standards or regulations, or mandated by any other reason (see subsection 6.3 below);
- Include the frequency, methods, responsibilities, scope, planning requirements and reporting, taking into consideration the importance of the processes concerned, any compliance timescale requirements, the

results of previous audits and incorporate the corresponding requirements to be agreed with the third-party auditors;

- Be submitted annually to the FEAR Committee for approval.

6.1.2. All audits shall be planned with sufficient advance to enable timely preparation of all parties involved and ensure that the impact on business operations is minimised.

6.1.3. The scope of audits shall be documented and validated.

6.2. Internal Audits

6.2.1. Criteria for Appointment of the Internal Auditors

The Internal Auditors shall be composed of one or more individuals that meet all the following criteria:

- Are able to preserve the independence of audits and conduct them in an objective and impartial manner;
- Possess sufficient qualifications and knowledge of information security.

The conducting of internal audits will be assigned to trusted, independent third parties. The assigned auditors shall meet the same criteria outlined above for internal auditors and follow the methodology outlined in section 6.2.2 (below), i.e. in practice conduct the audits as if they were members of an Internal Audit function.

6.2.2. Methodology for Internal Audits

Internal audits shall:

- Follow auditing best practice;
- Be supported by:
 - Appropriate checklists, aligned (where applicable) to the specific regulations or frameworks against which the audits are being conducted (e.g., ISO 27001:2022);
 - Established internal audit report templates;
- Take into consideration any documented outcomes of previous audits;
- Include the assessment of whether previously identified corrective actions have been implemented.

Except when otherwise dictated by a specific regulation or framework, internal audits shall use the following three-point scale for rating the findings:

Rating	Criteria
Compliant	The requirements are being met to an acceptable level.
Partially compliant	The requirements are just being met, but additional improvement is thought appropriate to bring the compliance to a level at which it can easily be maintained. Future audits will expect to see some degree of improvement.
Non-compliant	The requirements are not being met to an acceptable level, due to one or more issues identified. Remedial action must be taken to ensure that an acceptable level of compliance is achieved.

The findings of an internal audit shall be documented in an internal audit report and initially reported to:

- The head(s) of the audited function(s), requesting them to validate the accuracy of the findings
- The IT Manager

Any disagreement about findings of the report shall be resolved by the IT Manager, with escalation to The Board if necessary. The finalised report shall be shared with the FEAR Committee.

All the relevant records related to internal audits shall be retained as documentary evidence of the internal audit process.

6.3. External Audits

6.2.3. External information security audits can be any of the following:

- Audits mandated by regulatory bodies (e.g., data protection audits mandated by a relevant data protection authority);
- Audits required for certification (or re-certification) against a specific standard that the OCA has decided to apply for (or renew);
- Audits done by or on behalf of the OCA's clients and established in contractual terms with them;

6.2.4. External audits shall be conducted by the designated external auditors, using their own methodologies and supporting tools / checklists / templates.

6.2.5. A main contact shall be appointed for each external audit and be responsible for making arrangements with the external auditors for interviews and provision of evidentiary documentation, in liaison with the head(s) of the function(s) in scope for the audit (or their delegate(s)).

6.2.6. Reports from external audits shall be shared with:

- The head(s) of the audited function(s);

- The IT Manager;
- The FEAR Committee.

7. Nonconformities and Opportunities for Improvement

- 7.1. In most cases, nonconformities and opportunities for improvement of information security policies, processes and controls are identified through audits (internal or external). However, they can also be identified by any members of staff, as part of their day-to-day work, and in that case, they should report them to the IT Manager for assessment.
- 7.2. All nonconformities identified in audits, as well as those reported by members of staff and assessed as relevant by the IT Manager, in liaison with Information Security, shall:
- Be evaluated and have appropriate corrective actions identified to address them, by Information Security in liaison with the relevant business functions;
 - Be recorded, with the relevant details, in a centralised nonconformity register;
 - Have assigned ownership and agreed timelines for implementation of the associated corrective actions;
 - Have the associated corrective actions reviewed and signed off by the IT Manager, and tracked to completion;
 - If they may correspond to either a new information security risks which had not been previously assessed, or information security risks that may need to be reassessed, be flagged for appropriate action as part of the risk management process. (See the [Information Security Risk Management Policy](#) for more information.)
- 7.3. Corrective actions shall be:
- Appropriate to the effects of the nonconformities encountered;
 - Appropriately documented;
 - Have timelines for implementation appropriate to the assessed risk and priority.

The same principles shall be applied to identified opportunities for improvement, although generally their implementation may be of lower priority than for addressing nonconformities, and timelines assigned accordingly.

See also the [Information Security Management System \(ISMS\) Policy](#).

8. Metrics and Reporting

- 8.1. Relevant metrics for information security audit and compliance monitoring shall be defined, and regularly obtained and reported by the IT Manager to the FEAR Committee.
- 8.2. Analysis of metrics shall be used to assess the efficiency of the information security audit and compliance monitoring processes and continuously improve them.

9. Policy Review Date

- 9.1. This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection, or any other significant changes in the organisation or its context that may dictate the need for an update.

10. Appendix A – Audit Definitions

	Internal Audit	External Audit
Purpose	To review and improve the efficiency and effectiveness of an organisation's operations and internal controls	To provide an independent opinion on the truthfulness and fairness of the organisation's adherence to financial, regulatory or legal requirements.
Conducted by	Employees of the organisation, typically from a dedicated internal audit department or independent third parties on the organisation's behalf	Independent auditors from outside the organisation
Scope	Determined by the organisations management	Defined by statutory requirements and regulations
Frequency	Ongoing and continuous process	Conducted annually or in-line with statutory and regulatory requirements
Reporting	Findings are reported to the organisations management	Findings are reported to external stakeholders such as shareholders, creditors and regulatory bodies
Obligation	Voluntary, based on the organisations needs or set requirements	Mandatory for most organisations to comply with legal and regulatory requirements

11. Document Control

Document Control	
Title:	Information Security Audit and Compliance Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

11.1. Document Revision History

Version	Date	Author	Summary of changes
0.1			Initial draft
1.0	06/11/2025	Dean Humphreys	Final revisions approved and version updated to 1.0 for release