Audit Portal

Audit Report

ISO 27001:2022 — Clause 7 Support

REFERENCE NUMBER **AUD-202603-9021**	AUDIT DATE **13 March 2026**
DEPARTMENT **People**	AUDITOR **Reuben Thomas**
CONTACT **Snadra Harris**	LOCATION **Remote**
STATUS **Completed**	REPORT DATE **26 March 2026**

Compliance Score

71%

Executive Summary

High-level snapshot of the audit results.

MNC	NC	OFI
1	1	1
Major Non-Conformances	Minor Non-Conformances	Opportunities for Improvement

Total Questions	7
Evidence Collected	2 files
Total Non-Conformances	3
Status	Completed

Non-Conformances & Findings

Detailed breakdown grouped by severity.

Major Non-Conformances (MNC)

MNC

High

Document control

Related to: 7.5.2 Documented information - Creating and updating

Document control across the ISMS-related documents appears to be incomplete, with some documents missing control tables entirely.

RECOMMENDATION

The organisation should consider extending formal document control requirements to all ISMS-relevant local procedures and operational guidance to improve consistency and reduce the risk of uncontrolled documents being used.

Status: Open | Target Date: 23 May 2026

Minor Non-Conformances (NC)

NC

High

Communication examples

Related to: 7.4 Communication

The organisation has not fully determined and documented ISMS-related communication requirements as required by Clause 7.4. While communication activities do occur, there was insufficient documented evidence showing a complete and structured determination of what to communicate, when to communicate, with whom, and who is responsible across the full scope of the ISMS.

RECOMMENDATION

Create a communication matrix that shows the what, when, with whom and who is responsible for ISMS related communications

Status: Open | Target Date: 22 April 2026

Opportunities for Improvement (OFI)

OFI

Medium

Single point of failure

Related to: 7.1 Resources

The organisation may benefit from further formalising resource contingency arrangements where key security or compliance activities are dependent on a single individual. This would improve resilience and reduce the risk of delays during periods of absence or staff change.

RECOMMENDATION

formalise resource contingency arrangements where key security or compliance activities are dependent on a single individual.

Status: In Progress | Target Date: 25 March 2026

Audit Summary

Question-by-question evidence and commentary.

1. 7.1 Resources

REQUIREMENT

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

CRITICAL

Answer: Compliant

NOTES & EVIDENCE

Notes

The organisation demonstrated that resources required for the establishment, implementation, maintenance and continual improvement of the ISMS had been considered at both operational and management levels. During the audit, management explained that information security activities are primarily coordinated by the IT Manager and supported by department heads, with additional specialist support procured externally where required. Budget allocation for core security tooling, staff awareness training, device management and external consultancy had been approved through the annual business planning cycle.

It was evident that resources have generally been made available in proportion to the size and complexity of the organisation. Management was able to describe how resource needs are reviewed during management review meetings and in response to business change, including growth in user numbers and adoption of additional cloud services. While the overall approach appeared adequate, some reliance remains on a small number of key individuals for ISMS administration and security oversight.

Evidence seen:

• ISMS budget / business planning document

• Management review meeting minutes

• Interview with IT Manager and Operations Manager

• List of active security tools and subscriptions

• Organisational chart showing security-related responsibilities

Evidence

No evidence uploaded.

2. 7.2 Competence

REQUIREMENT

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

HIGH

Answer: Compliant

NOTES & EVIDENCE

Notes

The organisation was able to demonstrate that competence requirements had been identified for relevant roles affecting information security performance. Core roles such as IT administration, HR, senior management and system owners had a clear understanding of their responsibilities, and staff interviewed were generally able to explain their involvement in protecting information assets. Mandatory awareness training is issued to personnel, and role-specific knowledge is developed through practical experience, supplier-led sessions and external certifications where appropriate.

Training records sampled showed that most personnel had completed baseline information security awareness training. The organisation also retains evidence of qualifications and experience for individuals holding specialist positions. However, while competence appears to exist in practice, the method used to define and periodically review role-specific competence requirements was not consistently formalised across all functions. This was particularly evident for personnel with responsibility for supplier management and data handling within operational teams.

Evidence seen:

• Staff training matrix

• Information security awareness training completion records

• HR personnel files with qualifications / training evidence

• Interviews with selected staff members

• Job descriptions for key roles

Evidence

• Example.jpg

3. 7.3 Awareness

REQUIREMENT

Persons doing work under the organization’s control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved

information security performance; and

c) the implications of not conforming with the information security management system requirements.

CRITICAL

Answer: Compliant

NOTES & EVIDENCE

Notes

The audit found that employees were generally aware of the organisation’s information security expectations and understood the importance of following policies and reporting concerns. Staff interviewed could describe the purpose of password controls, phishing awareness, incident reporting routes and acceptable use requirements. Awareness activities are supported through induction training, periodic refresher sessions and internal communications distributed by management.

There was also evidence that personnel understood that nonconformity with information security requirements could have consequences for both the business and individuals. This included reputational harm, regulatory exposure and possible disciplinary outcomes where deliberate or negligent breaches occur. Although staff awareness levels sampled were broadly positive, the organisation’s approach remains somewhat reliant on periodic training rather than a more structured year-round awareness programme with measurable outcomes.

Evidence seen:

• Security awareness training slides / e-learning records

• Induction checklist

• Staff interviews

• Internal awareness emails / posters / communications

• Incident reporting guidance

Evidence

No evidence uploaded.

4. 7.4 Communication

REQUIREMENT

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate.

CRITICAL

Answer: Non-Compliant

NOTES & EVIDENCE

Notes

The organisation has identified a range of internal and external communications relevant to the ISMS, including escalation of incidents, management reporting, policy communication, client communications where required, and engagement with external suppliers. Internal communications are primarily handled through email, team meetings and management-led updates, while external communication responsibilities sit with management, IT, and relevant service owners depending on the nature of the matter.

Whilst communication takes place in practice, the audit identified that the organisation's communication arrangements were only partially defined in documented form. The audit team saw examples of communication occurring appropriately, but there was limited evidence of a consolidated communication framework setting out what will be communicated, by whom, when, and through which channels for all key ISMS-related scenarios. This could reduce consistency during periods of disruption or security incidents.

Evidence seen:

• Incident response procedure

• Internal emails communicating policy updates

• Management meeting minutes

• Interview with management and IT personnel

• Customer / supplier communication examples

Evidence

No evidence uploaded.

5. 7.5.1 Documented information - General

REQUIREMENT

The organization’s information security management system shall include:

a) documented information required by this document; and

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

CRITICAL

Answer: Compliant

NOTES & EVIDENCE

Notes

The organisation has established a set of documented information to support the operation of the ISMS, including policies, procedures, risk assessment outputs, treatment plans, audit records, management review outputs and selected operational records. Documentation sampled was generally relevant to the organisation’s activities and aligned with the scope of the ISMS. Management showed awareness of which documents form part of the mandatory and operational ISMS set.

The level of documented information appeared broadly appropriate to the size and nature of the organisation. In practice, the organisation does not appear overburdened by excessive documentation and has focused on producing materials that support operation of the ISMS. However, there were some inconsistencies in how supporting records were referenced across departments, with some locally maintained records not clearly linked back to central ISMS control documentation.

Evidence seen:

• ISMS policy suite

• Risk assessment and treatment records

• Internal audit schedule and reports

• Management review records

• Document register / shared document repository

Evidence

No evidence uploaded.

6. 7.5.2 Documented information - Creating and updating

REQUIREMENT

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

CRITICAL

Answer: Non-Compliant

NOTES & EVIDENCE

Notes

Sampled documented information generally included suitable identification and description, such as titles, dates, version numbers and authorship or ownership. Templates used for policies and procedures appeared standardised, supporting consistency in document presentation and review. Where documents had been recently updated, there was usually evidence that the change had been reviewed and reissued through the organisation's normal document management process.

However, the audit noted that not all supporting operational documents followed the same standard. A small number of locally maintained procedures and working documents lacked consistent version control or formal approval references. While this did not appear to undermine overall ISMS operation, it introduces a risk that outdated or unofficial information could be used if local documents are not adequately controlled.

Evidence seen:

• Policy and procedure templates

• Version-controlled documents in shared repository

• Approval records / document headers

• Sample departmental working instructions

• Interviews with document owners

Evidence

No evidence uploaded.

7. 7.5.3 Documented information - Control of documented information

REQUIREMENT

Documented information required by the information security management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). For the control of documented

information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

CRITICAL

Answer: Compliant

NOTES & EVIDENCE

Notes

Documented information is primarily stored electronically within shared systems with access permissions applied according to role and business need. The organisation demonstrated that core ISMS documentation is retained within centrally managed repositories, with editing rights restricted to authorised personnel. Backups, retention arrangements and access controls for these systems were described during interview and supported by system configuration evidence where sampled.

Retention and protection arrangements appear generally suitable, though the audit identified some inconsistency in archival and disposal practices for obsolete documents. Superseded versions of controlled documents were not always clearly marked to prevent unintended use, and one sampled departmental procedure remained accessible in a shared area despite having been replaced by a newer version. This indicates that control of documented information is mostly effective, but not fully consistent across all repositories.

Evidence seen:

• Shared document repository structure

• Access permissions for ISMS folders

• Sample controlled documents and archived versions

• Backup overview / IT administration explanation

• Retention and deletion arrangements where defined

Evidence

• Example.jpg