ISO 27001:2022 Compliance Audit Report

Prepared for: ISOGUARD_Test

Report Date: February 17, 2026

Report Type	ISO 27001:2022 Compliance Assessment
Standard	ISO/IEC 27001:2022
Generated By	ISOGUARD AI Analysis Engine
Report Version	1.0

Disclaimer: This report is generated by AI-assisted analysis and should be reviewed by qualified information security professionals. The findings and recommendations are based on the documents provided and may not represent a complete assessment of the organization's information security posture.

Executive Summary

This report presents the results of an ISO 27001:2022 compliance assessment covering **1 Annex A control categories**. The assessment was performed using AI-powered document analysis to evaluate the organization's information security management system (ISMS) against the requirements of ISO/IEC 27001:2022.

Overall Compliance Score	34%
Checklists Analyzed	**1**
Compliant	**0**
Partially Compliant	**1**
Non-Compliant	**0**

Checklist Results Overview

Checklist	Status	Score	Gaps
A.5 Information Security Policies	■ Partial	34%	6

A.5 Information Security Policies

Compliance Status	**Partial**
Compliance Score	**34%** ■■■■■■■■■■

Summary

The audit report provides evidence that an information security policy framework exists and that information security is considered in project management, with senior management oversight. However, several mandatory elements of ISO 27001:2022 A.5 are not clearly evidenced (approval/sign-off, explicit definition, exception procedures, segregation of duties, and external contact/threat intelligence processes).

Control Scores

Control	Score	Progress
A.5.7_Threat_intelligence	0%	■■■■■■■■■■
A.5.3_Segregation_of_duties	0%	■■■■■■■■■■
A.5.5_Contact_with_authorities	0%	■■■■■■■■■■
A.5.4_Management_responsibilities	50%	■■■■■■■■■■
A.5.1_Policies_for_information_security	60%	■■■■■■■■■■
A.5.6_Contact_with_special_interest_groups	0%	■■■■■■■■■■
A.5.8_Information_security_in_project_management	100%	■■■■■■■■■■
A.5.2_Information_security_roles_and_responsibilities	60%	■■■■■■■■■■

Key Findings

1. Evidence of documented information security policies and alignment with strategy: the Executive Summary states 'In line with the strategic direction of the organisation and the intended results of the Information Security Management System...' and the report highlights 'Excellent starter signed documentation covering all aspects of IS policies and requirements prior to the start date'.

2. Information security considered in projects: the Executive Summary explicitly lists 'IS consideration in project management' as a positive finding and the assessment included interviews with the Senior Project Manager (Tim Kitchener), indicating this control (A.5.8) is implemented.

3. Partial evidence of roles and responsibilities: the report includes numerous interviewees and references to 'role-based assignment' areas and also identifies an opportunity to 'add specific clauses on information security to the Relationship Manager responsibilities', indicating roles exist but are not comprehensive or fully documented.

4. Policy approval and control weakness: a minor nonconformity was raised because 'the ISMS documentation was updated in “draft status” reflecting the new HCPC Management Structure, rather than being incorrect but signed off' — this shows lack of consistent policy sign-off/approval and control of published document versions.

5. Legal and regulatory linkage: the report contains a 'Legislation and compliance. A.18' section and prior nonconformity shows a maintained list of legislation (REC 18) — evidence that applicable laws/regulations are considered, although earlier a previous issue existed and was corrected.

6. Gaps in operational controls and governance: prior and current findings include access rights reviews not consistently performed and BCP not tested for a year, showing weaknesses in management responsibilities and operationalisation of policy provisions.

Identified Gaps

■ **1.** A.5.1 — No explicit evidence in the report that the IS policy contains a clear organisational definition of 'information security', or an explicit exceptions/exemptions procedure; the 'draft status' ISMS documentation issue indicates gaps in policy approval and publication.

■ **2.** A.5.3 — Segregation of duties: the report does not document a formal segregation of duties review or controls to manage role conflicts; no mapping of duties or compensating controls is presented.

■ **3.** A.5.5 — Contact with authorities: there is no documented process or evidence showing formal contact points or procedures for liaising with legal, regulatory or law enforcement authorities in the report.

■ **4.** A.5.6 — Contact with special interest groups: the report does not show membership, participation or formal engagement with industry special interest groups or information sharing communities.

■ **5.** A.5.7 — Threat intelligence: no evidence of a threat intelligence process (collection, analysis, distribution) or how emergent threats feed into the risk management process is presented.

■ **6.** A.5.4 / management responsibilities — while management commitment is referenced, there is insufficient evidence that management has approved the IS policy in its current structure, or that role responsibilities have been updated and signed-off following the management restructure (drafts present).

Recommendations

→ **1.** Finalize and formally approve the ISMS policy and related topic-specific policies (incident management, asset management, network security, secure development). Replace any 'draft' status documents with signed/dated versions and maintain an auditable document control record (approver, date, version).

→ **2.** Update policies to explicitly include the ISO 27001:2022 A.5 required statements: a clear definition of information security for the organisation, a framework for setting/measuring information security objectives, guiding principles, explicit commitment to legal/contractual compliance, commitment to continual improvement of the ISMS, role-based assignments, and a documented exceptions/exemptions procedure.

→ **3.** Perform a formal segregation of duties review: map critical processes and systems, identify conflicting responsibilities (e.g., development/test/production, change approval vs implementer, user provisioning vs access reviewer), and implement mitigating controls or revise role descriptions where conflicts exist.

→ **4.** Establish and document processes for external engagement: define and record points of contact with relevant authorities (regulatory, law enforcement), membership/engagement with special interest groups, and formalise a threat intelligence intake process (sources, owners, frequency, how intelligence feeds into risk treatment).

→ **5.** Remediate operational shortfalls identified by the auditor: implement periodic access rights reviews (documented evidence and schedule), change HR key safe PIN immediately and set recurring change schedule, and test the business continuity plan promptly (especially after DR site relocation).

Auditor Comments

• The audit report is thorough in identifying nonconformities and opportunities for improvement and documents evidence across many ISO domains; however, it is written against ISO/IEC 27001:2013 and some 2022-specific controls (A.5.5–A.5.7) are not explicitly addressed in the evidence provided.

• The report contains useful operational findings (access control, BCP, HR key safe) and prior closure activity (legislation list corrected), but does not provide sufficient artefacts proving completed remediation or the presence of formal policies covering exceptions, threat intelligence, and segregation of duties.

• To strengthen audit evidence for A.5, include the approved policy documents (with approver and date), role descriptions updated for the management restructure, an exceptions register, records of external engagements (letters/MoUs/meeting minutes), and the threat intelligence intake and handling procedures.

Consolidated Recommendations

The following is a consolidated list of recommendations across all analyzed control categories. These should be prioritized based on risk and business impact.

A.5 Information Security Policies

R1. Finalize and formally approve the ISMS policy and related topic-specific policies (incident management, asset management, network security, secure development). Replace any 'draft' status documents with signed/dated versions and maintain an auditable document control record (approver, date, version).

R2. Update policies to explicitly include the ISO 27001:2022 A.5 required statements: a clear definition of information security for the organisation, a framework for setting/measuring information security objectives, guiding principles, explicit commitment to legal/contractual compliance, commitment to continual improvement of the ISMS, role-based assignments, and a documented exceptions/exemptions procedure.

R3. Perform a formal segregation of duties review: map critical processes and systems, identify conflicting responsibilities (e.g., development/test/production, change approval vs implementer, user provisioning vs access reviewer), and implement mitigating controls or revise role descriptions where conflicts exist.

R4. Establish and document processes for external engagement: define and record points of contact with relevant authorities (regulatory, law enforcement), membership/engagement with special interest groups, and formalise a threat intelligence intake process (sources, owners, frequency, how intelligence feeds into risk treatment).

R5. Remediate operational shortfalls identified by the auditor: implement periodic access rights reviews (documented evidence and schedule), change HR key safe PIN immediately and set recurring change schedule, and test the business continuity plan promptly (especially after DR site relocation).

Next Steps: Review the findings and recommendations with your information security team. Develop an action plan to address identified gaps and improve your overall compliance posture. Consider engaging qualified ISO 27001 auditors for a formal certification assessment.