ResolvX

Internal Audit Report

ISMS Internal Audit - Q1 2026

AUDIT-RPT-001 - v1.0 - 2026 - Internal - Confidential

Document Information

Document ID	AUDIT-RPT-001
Version	1.0
Audit Period	Q1 2026 - January to March 2026
Audit Type	ISO 27001:2022 Clause 9.2 Internal Audit
Lead Auditor	GRC Lead - Derick G. Dmello
Observer / Approver	CISO
Audit Scope	Full ISMS scope: all ResolvX information assets, processes, controls, and personnel
Framework	ISO 27001:2022 Annex A - SOC 2 TSC CC1-CC9 - NIST CSF 2.0
Audit Checklist Reference	AUDIT-CL-001
CAP Reference	AUDIT-CAP-001
Classification	Internal - Confidential

1. Executive Summary

ResolvX conducted its first formal internal ISMS audit in Q1 2026, covering 31 ISO 27001:2022 Annex A controls and 17 SOC 2 Trust Service Criteria across all programme phases (Phases 1-4). The audit was conducted by the GRC Lead in accordance with ISO 27001:2022 Clause 9.2 and ISO 27003:2017 guidance on internal audit.

The overall audit result is SATISFACTORY. ResolvX has established a comprehensive ISMS across all key control domains within its first programme year. No major nonconformities were identified. Five minor nonconformities and three observations were raised, all of which have been incorporated into the Corrective Action Plan (AUDIT-CAP-001) with defined owners and deadlines.

Finding Type	ISO 27001	SOC 2	Total
Conformant	22	15	37
Minor Nonconformity	4	1	5
Major Nonconformity	0	0	0
Observation	3	0	3

Overall Audit Verdict: SATISFACTORY - ISMS is fit for purpose at current maturity stage. No certification blocking findings.

2. Audit Scope and Methodology

2.1 Scope

This audit covered the full ISMS scope as defined in the ResolvX Programme Foundation (Phase 1). The scope includes:

- All information assets classified under POL-004 (Public, Internal, Confidential, Restricted).
- All ResolvX personnel, contractors, and third parties with access to ResolvX systems.
- Cloud infrastructure (AWS eu-west-1, eu-central-1).
- All corporate SaaS applications in the vendor register.
- All policies (POL-001 to POL-006), the Incident Response Plan, and vendor risk artefacts.
- Processes: risk management, access control, vendor risk, incident response, privacy, change management.

2.2 Methodology

The audit was conducted using a risk-based approach aligned to ISO 27001:2022 Clause 9.2 and ISO/IEC 27003:2017 Section 9.2. Audit methods included:

- Document review: policies, procedures, registers, and artefacts from Phases 1-4.
- Interview: GRC Lead, Head of Cloud Ops, IT Admin, DevSecOps Engineer.
- Observation: system configuration reviews (Okta, AWS, Jamf, Snyk, GitHub).
- Sampling: access reviews (5 leavers), document classification (10 documents), training records (20 employees).
- Technical testing: MFA enforcement verification, TLS configuration check, S3 encryption confirmation.

2.3 Audit Criteria

Controls were assessed against: ISO/IEC 27001:2022 Annex A requirements; SOC 2 Trust Service Criteria (AICPA 2017); ResolvX information security policies (POL-001 to POL-006); NIST CSF 2.0 applicable subcategories; applicable legal and regulatory requirements (GDPR, Irish DPC guidance).

3. Audit Findings

3.1 Minor Nonconformities

The following five minor nonconformities were identified. Each has a corresponding corrective action in AUDIT-CAP-001.

A5.12 / POL-004 - Data Classification Labelling

NC-001	Minor NC	2 of 10 sampled documents lacked classification labels. POL-004 requires all documents to carry a classification label at creation. The policy was published but the labelling workflow was not operationalised in Google Workspace document templates.
Root Cause	**Action Required**	
POL-004 published without corresponding template updates or workflow enforcement	Add classification labels to Workspace templates; retrain document owners; re-test sample (F-001)	See CAP Register AUDIT-CAP-001 for owner, due date, and verification method

A5.17 / CC6.1 - Hardware Key Enforcement for Admin Accounts

NC-002	Minor NC	POL-003 and the vendor assessment framework require hardware FIDO2 keys for privileged account authentication. Okta policy for the admin group has not yet been updated to enforce hardware key requirement - 8 admin accounts still using TOTP-based MFA only.
Root Cause	**Action Required**	
Hardware key procurement delayed; Okta policy change deprioritised	Procure FIDO2 keys for all 8 admin accounts; update Okta admin group policy; verify enforcement (F-002)	See CAP Register AUDIT-CAP-001 for owner, due date, and verification method

A5.23 - SSO Coverage for Corporate SaaS

NC-003	Minor NC	2 legacy SaaS integrations in the vendor register are not connected to Okta SSO despite POL-005 requiring all corporate SaaS to authenticate via Okta. Both tools were onboarded before the SSO policy was formalised.
Root Cause	**Action Required**	
Tools onboarded pre-policy; migration deprioritised	Configure Okta SAML/OIDC for both tools; migrate authentication; update vendor register (F-003)	See CAP Register AUDIT-CAP-001 for owner, due date, and verification method

A6.3 / CC2.2 - Security Awareness Training Completion

NC-004	**Minor NC**	Annual security awareness training completion rate is 93% (112/120 employees). 8 employees are overdue beyond the 30-day grace period. POL-002 requires all staff to complete annual security awareness training.
Root Cause	**Action Required**	
No automated escalation when training is overdue; manager notification not triggered	Escalate to line managers for 8 overdue employees; configure LMS automation for future cycles (F-004)	See CAP Register AUDIT-CAP-001 for owner, due date, and verification method

A8.8 / CC7.1 - Vulnerability Patch SLA Compliance

NC-005	**Minor NC**	2 High severity findings in Snyk have been open for more than 30 days, exceeding the 30-day patch SLA defined in the Information Security Policy (POL-001). Both findings are tracked in Snyk but not assigned to an active engineering sprint.
Root Cause	**Action Required**	
Engineering sprint prioritisation did not include vulnerability backlog; no automated SLA escalation	Assign both findings to current sprint; configure Snyk-Jira integration for automated ticket creation on High findings (F-005)	See CAP Register AUDIT-CAP-001 for owner, due date, and verification method

3.2 Observations

The following three observations are not nonconformities but represent opportunities for improvement that will strengthen the ISMS as ResolvX scales.

A5.9 - Formal Asset Register

OBS-001	**Observation**	An asset inventory exists within the programme foundation documents but is not maintained as a standalone, formally controlled ISMS document with a defined review cycle and named owner. As ResolvX scales, a formal asset register will be increasingly important for scope management.
Root Cause	**Action Required**	
Asset inventory created as scoping artefact; not yet formalised as ISMS document	Formalise as standalone ISMS document with document ID, version control, named owner, and annual review (F-006)	See CAP Register AUDIT-CAP-001 for owner, due date, and verification method

A5.28 - Evidence Handling - Not Yet Field Tested

OBS-002	**Observation**	Evidence handling procedures are documented in IR-PLAN-001 Section 5 but have not been tested in a real P1/P2 incident or as a dedicated exercise inject. The Feb 2026 tabletop did not include evidence chain-of-custody as a specific test.
Root Cause	**Action Required**	
No P1/P2 incident to date; evidence handling not included in tabletop injects	Include evidence handling as a specific inject in Tabletop Exercise 2 (Aug 2026) (F-007)	See CAP Register AUDIT-CAP-001 for owner, due date, and verification method

A8.12 - DLP Coverage Scope

OBS-003	**Observation**	Current DLP controls are limited to Google Workspace email and Drive rules. There is no dedicated DLP tooling covering API traffic, S3 egress, or endpoint data exfiltration channels. At current scale this is acceptable, but as data processing volume grows, expanded DLP coverage should be assessed.
Root Cause	**Action Required**	
Current DLP scope deemed adequate at programme inception; not yet a material gap	Assess dedicated DLP tooling (AWS Macie, CASB); document residual risk if expansion deferred (F-008)	See CAP Register AUDIT-CAP-001 for owner, due date, and verification method

4. Positive Findings and Strengths

The following areas demonstrated strong control implementation and were rated Conformant with no gaps identified:

Policy Suite (A5.1)	All 6 policies (POL-001 to POL-006) are in place, approved by the CISO, and current. Policy coverage is comprehensive for a company at this maturity stage.
Vendor Risk Management (A5.19 / CC9.1-9.2)	Tier 1 vendor assessments completed for all 6 critical vendors; DPAs in place for all data-processing vendors; sub-processor register maintained. TPRM framework is audit ready.
Incident Response (A5.24-A5.27 / CC7.3-7.5)	IR plan, 3 runbooks, tabletop exercise, and incident log template all in place and tested. Tabletop findings remediated promptly. IR programme is strong for a first-year ISMS.
Access Control (A5.15 / CC6.1-6.7)	MFA enforced for 100% of users; RBAC via Okta; quarterly access review conducted; JML process implemented and evidenced. No unauthorised access found in sampled review.
Privacy Programme (A5.34)	ROPA covering 9 processing activities; DSR process documented; GDPR processor/controller distinction correctly implemented; breach notification procedures aligned to 72-hour GDPR obligation.
Cryptography (A8.24)	AES-256 at rest and TLS 1.3 in transit confirmed across all production systems. KMS key management in place. No unencrypted sensitive data storage identified.
Monitoring and Logging (A8.15-A8.16)	CloudTrail with integrity validation enabled across all AWS regions; Okta and Datadog monitoring active; alert review cadence documented.

5. Conclusion and Recommendations

Overall Audit Verdict: SATISFACTORY

ResolvX has successfully established a comprehensive ISMS in its first programme year. The control framework covers all required domains under ISO 27001:2022 and SOC 2 Trust Service Criteria. The absence of major nonconformities is notable for a first internal audit and reflects the quality and completeness of the Phase 1-4 programme deliverables.

The five minor nonconformities identified are all addressable within the Q2 2026 timeframe and do not represent systemic weaknesses. The three observations are forward-looking improvements appropriate for a programme in growth stage.

5.1 Recommendations for Phase 6

- Close all 5 minor nonconformities before initiating any external SOC 2 readiness assessment
- Formalise the asset register (OBS-001) before external audit scope is defined
- Include evidence handling in Tabletop Exercise 2 (OBS-002)
- Commission an external gap assessment against SOC 2 Type II criteria before selecting an audit firm
- Consider a limited-scope penetration test to validate technical controls ahead of Phase 6

6. Document Control

Document ID	AUDIT-RPT-001
Version	1.0
Audit Date	Q1 2026
Report Date	2026-03-31
Prepared By	GRC Lead - Derick G. Dmello
Reviewed By	CISO
Classification	Internal - Confidential
Retention	5 years
Next Audit	Q1 2027 (annual cycle) - or sooner if significant ISMS change
Related Documents	AUDIT-CL-001 (Checklist) - AUDIT-CAP-001 (CAP) - AUDIT-SOC2-001 (SOC 2 Readiness)

Role	Name	Signature / Date
Lead Auditor / GRC Lead	Derick G. Dmello	
Approver / CISO		