ResolvX

SOC 2 Type II Readiness Assessment

Trust Service Criteria - Gap Analysis and Readiness Scoring

AUDIT-SOC2-001 - v1.0 - 2026 - Internal - Confidential

Document Information

Document ID	AUDIT-SOC2-001
Version	1.0
Assessment Date	Q1 2026
Prepared By	GRC Lead - Derick G. Dmello
Reviewed By	CISO
Purpose	Pre-audit SOC 2 Type II readiness scoring to identify gaps before engaging an external audit firm
SOC 2 Standard	AICPA Trust Services Criteria for Security, Availability, and Confidentiality (2017)
Classification	Internal - Confidential
Next Step	Remediate open CAP actions; engage external audit firm H2 2026

1. Executive Summary

This SOC 2 Type II Readiness Assessment evaluates ResolvX's current control posture against the AICPA Trust Service Criteria (TSC) for Security (required), Availability, and Confidentiality. It is designed to identify remaining gaps before ResolvX engages an external audit firm for a formal SOC 2 Type II examination.

Overall SOC 2 Readiness Rating: SUBSTANTIALLY READY

ResolvX has implemented controls covering all nine SOC 2 TSC families (CC1-CC9). The readiness assessment identified 15 criteria as Fully Ready, 2 as Partially Ready (minor gaps), and 0 as Not Ready. The primary gaps align with the minor nonconformities identified in the Q1 2026 internal audit (AUDIT-RPT-001) and are tracked in the CAP (AUDIT-CAP-001). Subject to CAP remediation, ResolvX is on track for a SOC 2 Type II observation period in H2 2026.

TSC Family	Fully Ready	Partial	Overall
CC1 - Control Environment	2/2	—	Ready
CC2 - Communication & Information	1/2	1	Partial - training gap
CC3 - Risk Assessment	2/2	—	Ready
CC4 - Monitoring of Controls	2/2	—	Ready
CC5 - Control Activities	2/2	—	Ready
CC6 - Logical & Physical Access	5/6	1	Partial - hardware key gap
CC7 - System Operations	4/5	1	Partial - vuln SLA gap
CC8 - Change Management	2/2	—	Ready
CC9 - Risk Mitigation	2/2	—	Ready

2. Readiness by TSC Family

CC1 - Control Environment

Readiness Status: Ready

Criteria Tested:

- CC1.1 - COSO Principle 1: Commitment to integrity and ethical values
- CC1.3 - Organisational structure and accountability

Strengths:

Policies (POL-001 to POL-006) establish the ethical and governance framework. Controls Owners Register documents accountability. CISO approval of all policies evidence leadership commitment.

CC2 - Communication and Information

Readiness Status: Partially Ready

Criteria Tested:

- CC2.1 - Information quality and use
- CC2.2 - Internal communication of IS requirements

Strengths:

Risk register, gap analysis, and control matrices provide quality information inputs. Internal communication channels established.

Gaps and Required Evidence:

- CC2.2: Security awareness training completion 93% - 8 employees overdue. CAP action F-004 targets 100% completion by 2026-04-01. Evidence required: LMS completion report at 100%.

CC3 - Risk Assessment

Readiness Status: Ready

Criteria Tested:

- CC3.1 - Risk assessment process
- CC3.2 - Risk identification and assessment

Strengths:

Comprehensive risk register (Phase 2) with likelihood/impact scoring, heat map, and treatment plans. Risk methodology documented. Annual review cycle established.

CC4 - Monitoring of Controls

Readiness Status: Ready

Criteria Tested:

- CC4.1 - Ongoing monitoring
- CC4.2 - Evaluation and communication of deficiencies

Strengths:

Datadog, GuardDuty, and Okta monitoring active. Internal audit programme established (AUDIT-CL-001). CAP process tracks deficiencies to resolution.

CC5 - Control Activities

Readiness Status: Ready

Criteria Tested:

- CC5.1 - Control selection and development
- CC5.2 - Technology controls

Strengths:

Control matrix maps ISO 27001 Annex A and SOC 2 TSC to implemented controls. Technology controls verified during audit.

CC6 - Logical and Physical Access

Readiness Status: Partially Ready

Criteria Tested:

- CC6.1 - Logical access security
- CC6.2 - New account provisioning
- CC6.3 - Access removal
- CC6.6 - External access restrictions
- CC6.7 - Data in transit protection
- CC6.8 - Malware protection

Strengths:

Comprehensive access control framework in place. MFA enforced for 100% of users. RBAC via Okta. Quarterly access reviews conducted. JML process implemented.

Gaps and Required Evidence:

- CC6.1 gap: Hardware FIDO2 key enforcement not yet configured in Okta for 8 admin accounts. CAP action F-002 targets completion by 2026-04-30. Evidence required: Okta admin group policy screenshot confirming hardware key enforcement.

CC7 - System Operations

Readiness Status: Partially Ready

Criteria Tested:

- CC7.1 - Vulnerability management
- CC7.2 - System monitoring
- CC7.3 - Incident evaluation
- CC7.4 - Incident response
- CC7.5 - Incident recovery

Strengths:

Strong system operations controls. Monitoring stack active. IR programme comprehensive and tested. Backup restoration verified.

Gaps and Required Evidence:

- CC7.1 gap: 2 High severity Snyk findings open >30 days, exceeding 30-day patch SLA. CAP action F-005 targets remediation by 2026-03-31. Evidence required: Snyk report showing 0 open High findings >30 days.

CC8 - Change Management

Readiness Status: Ready

Criteria Tested:

- CC8.1 - Change management process
- CC8.1(a) - Authorisation of changes

Strengths:

GitHub branch protection enforces PR-based change management. Code review mandatory. Deployment pipeline controls in place via GitHub Actions.

CC9 - Risk Mitigation

Readiness Status: Ready

Criteria Tested:

- CC9.1 - Vendor risk management
- CC9.2 - Vendor monitoring

Strengths:

Comprehensive TPRM framework (Phase 3). 14 vendors registered. All Tier 1 vendors assessed. DPAs and security clauses in all relevant contracts. Annual review cycle.

3. Pre-Audit Readiness Checklist

The following actions must be completed before engaging an external SOC 2 audit firm for a Type II observation period:

#	Action	Owner	Target Date	Status
1	Close CAP F-002 (hardware key enforcement)	IT Admin	2026-04-30	**Open**
2	Close CAP F-004 (training completion 100%)	GRC Lead + HR	2026-04-01	**In Progress**
3	Close CAP F-005 (Snyk High findings)	DevSecOps	2026-03-31	**Open**
4	Close CAP F-003 (SSO coverage)	IT Admin	2026-05-15	**Open**
5	Formalise asset register (CAP F-006)	GRC Lead	2026-06-30	**Open**
6	Define observation period start date with audit firm	CISO + GRC Lead	2026-07-01	**Planned**
7	Select external audit firm (Big 4 or specialist SOC 2 firm)	CISO	2026-06-01	**Planned**
8	Prepare evidence library for auditor access	GRC Lead	2026-07-01	**Planned**
9	Pre-audit walkthrough with selected audit firm	GRC Lead + CISO	2026-07-15	**Planned**
10	SOC 2 Type II observation period begins (target: 6 months)	All IRT	2026-08-01	**Planned**

4. Recommended SOC 2 Type II Timeline

Period	Phase	Key Activities
Q2 2026 (Apr - Jun)	**Remediation**	Close all CAP actions. Formalise asset register. Select audit firm. Prepare evidence library.
Jul 2026	**Pre-audit walkthrough**	Engage selected audit firm. Pre-audit walkthrough to validate readiness. Agree observation period start date.
Aug 2026 - Jan 2027	**Observation Period**	SOC 2 Type II 6-month observation period. GRC Lead maintains control evidence. Monthly evidence collection checkpoints.
Feb 2027	**Audit Fieldwork**	Auditor performs testing and interviews. GRC Lead provides evidence responses.
Mar 2027	**Report Issuance**	SOC 2 Type II report issued. Distribute to clients under NDA.

5. Document Control

Document ID	AUDIT-SOC2-001
Version	1.0
Prepared By	GRC Lead - Derick G. Dmello
Reviewed By	CISO
Classification	Internal - Confidential
Retention	5 years
Related Documents	AUDIT-RPT-001 (Audit Report) - AUDIT-CAP-001 (CAP) - AUDIT-CL-001 (Checklist)