INFORMATION SECURITY

GAP ANALYSIS REPORT

ResolvX — GRC Compliance & Audit Readiness Programme

Phase 2: Risk & Controls | Version 1.0 | 2026

Frameworks	Owner	Classification	Review Cycle
ISO 27001 · SOC 2 · NIST CSF	GRC Lead — D. Dmello	Confidential	Quarterly

Executive Summary

This Gap Analysis Report synthesises findings across all three framework mappings completed in Phase 2 of the ResolvX GRC Programme - ISO/IEC 27001:2022, SOC 2 Trust Services Criteria, and NIST CSF 2.0. It identifies where control gaps exist, quantifies them by domain and severity, and produces the prioritised remediation roadmap that will drive Phases 3 through 5.

Aggregate Gap Picture

Framework	Total Controls	Implemented	Partial	Not Done	Gap %
ISO 27001:2022 Annex A	93	15 (16%)	48 (52%)	30 (32%)	84%
SOC 2 TSC (Security + Availability + Privacy)	44	6 (14%)	25 (57%)	13 (30%)	87%
NIST CSF 2.0	103	20 (19%)	39 (38%)	44 (43%)	81%

Programme Context

High gap percentages reflect a correct and honest baseline — not programme failure. The 16–19% implemented represents controls ResolvX already had. The 38–57% partial means most controls exist but need documentation and evidence. The 30–43% not done is the Phase 3–5 roadmap, already scoped and owned.

The Three Critical Gap Clusters

Across all three frameworks, the same three domains surface as critical gaps regardless of which lens is applied:

1 Detection & Response

No SIEM, no formalised IR Plan, no comprehensive alerting. An attacker bypassing preventive controls would operate undetected. Closes in Phase 4.

2 Policy & Governance

Policy suite not published. Without formal policies, SOC 2 CC5 and ISO 5.1 cannot be evidenced by an auditor. Closes in Phase 3.

3 Privacy & Compliance

No ROPA, no DSR process, GDPR data mapping incomplete. Drives the highest single FAIR ALE in the portfolio ($200K–$2M). Closes in Phase 3.

1. ISO 27001:2022 Gap Analysis

1.1 Gap Summary by Domain

Domain	Controls	Implemented	Partial	Not Done	Completion
5 — Organizational	37	6	19	12	16%
6 — People	8	2	5	1	25%
7 — Physical	14	5	7	2	36%
8 — Technological	34	2	17	15	6%
Total	93	15	48	30	16%

The Technological domain (8) has the lowest completion at 6% — foundational controls exist (MDM, MFA, EDR) but are not yet documented to audit standards. Physical (7) scores highest because ResolvX's cloud-native architecture means most physical controls are inherited from AWS, a documented scope exclusion.

1.2 Critical ISO 27001 Gaps

Control ID	Control Name	Gap Description	Risk Impact
5.1	Policies for information security	Policy suite not published	SOC 2 blocker; no governance foundation
5.18	Access rights	No quarterly access review process	RSK-004, RSK-022
5.19	Supplier relationships	No TPRM programme	RSK-011–RSK-015
5.24	Incident management planning	No IR Plan	RSK-001–RSK-005
5.26	Response to incidents	No IR runbooks	RSK-001–RSK-005
5.34	Privacy and protection of PII	No ROPA, no DSR process	RSK-017, RSK-019
8.2	Privileged access rights	No formal PAM programme	RSK-008
8.15	Logging	Application logging incomplete	RSK-010
8.16	Monitoring activities	SIEM not deployed	RSK-010
8.13	Information backup	Restoration not tested	RSK-001, RSK-007

1.3 ISO 27001 Remediation Priorities

Horizon	Controls	Focus Area
Q1 2026 — Immediate	5.1, 8.15, 8.16, 8.8	IS Policy; SIEM deployment; vulnerability management formalisation
Q2 2026 — 30–60 days	5.18, 5.19, 8.2, 8.3, 5.34	Access reviews; TPRM; PAM policy; Access control policy; ROPA/DSR
Q3 2026 — 60–90 days	5.24, 5.26, 8.13, 5.35	IR Plan; runbooks; backup restoration testing; internal audit programme

2. SOC 2 Trust Services Criteria Gap Analysis

2.1 Gap Summary by TSC Category

TSC	Category	Criteria	Implemented	Partial	Not Done	Status
CC1	Control Environment	5	1	4	0	Partial
CC2	Communication & Information	3	0	2	1	Partial
CC3	Risk Assessment	4	3	1	0	Strong
CC4	Monitoring Activities	2	0	0	2	Gap
CC5	Control Activities	3	0	1	2	Gap
CC6	Logical & Physical Access	8	3	5	0	Partial
CC7	System Operations	5	0	1	4	Gap
CC8	Change Management	1	0	1	0	Partial
CC9	Risk Mitigation	2	0	1	1	Partial
A1	Availability	3	1	2	0	Partial
P	Privacy	8	0	2	6	Gap
Total		44	6	25	13	

2.2 SOC 2 Audit Readiness Assessment

CC3 — Risk Assessment: Strongest Category

Phase 2 deliverables — Risk Methodology, Risk Register, Threat Landscape — satisfy CC3.1 through CC3.4 at a level that would withstand Type II audit scrutiny. This is the programme's most mature domain.

CC6 — Logical Access: Foundational but Incomplete

Okta MFA, AWS IAM RBAC, and EDR provide core technical controls. The gap is documentation — Access Control Policy, quarterly access reviews, and deprovisioning SLA. All Phase 3 deliverables.

CC4, CC5, CC7 — The SOC 2 Audit Blockers

These three categories would most likely cause a qualified or delayed Type II opinion if an audit were initiated today. CC7 alone has 4 Not Started criteria — no SIEM, no event triage, no IR Plan, no post-incident recovery procedures.

Privacy (P) — Enterprise Client Pipeline Risk

6 of 8 Privacy criteria Not Started. Enterprise clients in regulated industries will ask for evidence of privacy programme maturity during vendor due diligence. The entire P category is a Phase 3 priority.

2.3 Critical SOC 2 Gaps

TSC ID	Criterion	Gap Description	Phase to Close
CC4.1	Ongoing evaluations	No internal audit programme	Phase 5
CC5.3	Policy deployment	Policy suite not published	Phase 3
CC7.3	Event evaluation	No event triage process	Phase 4
CC7.4	Incident response	No IR Plan or runbooks	Phase 4
CC9.1	Vendor risk programme	No formal TPRM programme	Phase 3
P1.1–P8.1	Privacy (all criteria)	No ROPA, no DSR, no consent management	Phase 3

3. NIST CSF 2.0 Gap Analysis

3.1 Gap Summary by Function

Function	Subcategories	Implemented	Partial	Planned	Completion %
GV — Govern	31	8	10	13	26%
ID — Identify	18	7	6	5	39%
PR — Protect	22	9	10	3	41%
DE — Detect	11	1	6	4	9%
RS — Respond	13	0	2	11	0%
RC — Recover	8	0	3	5	0%
Total	103	25	37	41	24%

3.2 Function-Level Analysis

GV — Govern (26%) | New function in CSF 2.0

Phase 1 work satisfies GV.OC, GV.RR, and GV.RM at a level few organisations achieve at programme inception. Primary gaps: GV.PO (policy suite — Phase 3), GV.OV (oversight/internal audit — Phase 5), and GV.SC (supply chain risk — Phase 3).

ID — Identify (39%)

Strongest function relative to programme maturity. Risk assessment, asset management, and threat intelligence substantially covered through Phase 1–2 deliverables. Primary gap: ID.AM-07 (ROPA/GDPR data inventory — Phase 3).

PR — Protect (41%) | Highest completion rate

MFA, encryption at rest and in transit, and environment separation fully implemented. Primary gaps: formal access control policy (Phase 3), role-based training programme (Phase 3), and backup restoration testing (Phase 4).

DE — Detect (9%) | Critical gap

Most significant function-level gap in the programme. Only 1 of 11 subcategories fully implemented. The absence of SIEM means ResolvX cannot correlate events across sources. SIEM deployment is the single highest-leverage security investment on the roadmap.

RS — Respond (0%) | Phase 4 priority

Zero subcategories fully implemented — expected and planned. The entire Respond function is Phase 4 work: IR Plan, runbooks (ransomware, phishing, data breach), tabletop exercises, and regulatory notification procedures.

RC — Recover (0%) | Phase 4 priority

Technical recovery capability exists (multi-AZ, RDS backups) but is not formalised or tested. BCP, DR plan, and backup restoration testing are Phase 4 deliverables. RTO/RPO targets not yet defined.

3.3 NIST CSF 2.0 Target Profile

Tier	Description	ResolvX Status
Tier 1 — Partial	Ad hoc, reactive cybersecurity practices	← Current (Phases 1–2 complete)
Tier 2 — Risk-Informed	Risk-aware but not yet organisation-wide	← Target: Phase 3 complete
Tier 3 — Repeatable	Defined, consistently applied, reviewed	← Target: Phase 5 complete
Tier 4 — Adaptive	Continuously improving, threat-informed	Future: CCF / HITRUST Programme

4. Cross-Framework Gap Synthesis

4.1 The Control Gap Intersection

The following gaps are flagged Critical by all three frameworks simultaneously — highest-priority remediation items because they drive risk exposure, audit failure, and compliance penalties at the same time.

Gap Domain	ISO 27001	SOC 2 TSC	NIST CSF 2.0	Business Impact
Information Security Policy Suite	5.1 Not Started	CC5.3 Not Started	GV.PO-01 Planned	SOC 2 audit blocker; no governance foundation
SIEM / Centralised Monitoring	8.15, 8.16 Partial	CC7.1 Partial	DE.CM-01, DE.AE-03	Breach detection gap; attacker dwell time risk
Incident Response Plan	5.24, 5.26 Planned	CC7.3, CC7.4 Planned	RS.MA-01, RS.MI-01	No coordinated response to security events
TPRM Programme	5.19 Planned	CC9.1 Planned	GV.SC-01, GV.SC-04	Vendor risk uncontrolled; SOC 2 CC9 gap
Privacy Programme	5.34 Partial	P1–P8 Not Started	ID.AM-07 Planned	GDPR/CCPA enforcement risk; client friction
Quarterly Access Reviews	5.18 Planned	CC6.3 Partial	PR.AA-05 Partial	Lateral movement risk; SOC 2 CC6 gap
Internal Audit Programme	5.35 Planned	CC4.1 Planned	GV.OV-01 Planned	No independent assurance; SOC 2 CC4 gap
Backup Restoration Testing	8.13 Partial	A1.2 Partial	RC.RP-03 Planned	Untested recovery; unknown RTO/RPO

4.2 Gap Severity Summary

Priority	Gap Domains	Phase to Close	Estimated Effort
Critical	8 domains	Phase 3–4	High — policy, tooling, process design
High	14 domains	Phase 3–5	Medium — process formalisation + evidence
Medium	11 domains	Phase 4–6	Low-Medium — documentation + monitoring
Low	7 domains	Phase 6	Low — review cycles and maturity

5. Prioritised Remediation Roadmap

Phase 3 — Policy & Vendor Framework (Target: Q2 2026)

Phase 3 addresses the governance and policy foundation required before evidence collection can begin for SOC 2. Without policies there is nothing for an auditor to evaluate.

Deliverable	Frameworks Addressed	Gap Domains Closed
Information Security Policy	ISO 5.1 · SOC 2 CC5.3 · NIST GV.PO	Governance foundation
Acceptable Use Policy	ISO 5.10 · SOC 2 CC1.2 · NIST GV.PO	User conduct framework
Access Control Policy	ISO 5.15/5.18 · SOC 2 CC6.1 · NIST PR.AA	Access review cadence
Data Classification Policy	ISO 5.12 · SOC 2 CC6.1 · NIST PR.DS	Data handling framework
Vendor Management Policy + TPRM	ISO 5.19 · SOC 2 CC9.1 · NIST GV.SC	Vendor risk programme
Privacy Programme (ROPA + DSR)	ISO 5.34 · SOC 2 P1–P8 · NIST ID.AM-07	GDPR / CCPA compliance

Phase 4 — Incident Response & Detection (Target: Q3 2026)

Phase 4 closes the DE, RS, and RC function gaps in NIST CSF and the CC7 cluster in SOC 2.

Deliverable	Frameworks Addressed	Gap Domains Closed
SIEM Deployment	ISO 8.15/8.16 · SOC 2 CC7.1 · NIST DE.CM	Detection gap
Incident Response Plan	ISO 5.24/5.26 · SOC 2 CC7.3/CC7.4 · NIST RS	Response framework
IR Runbooks (×3 : ransomware, phishing, breach)	ISO 5.26 · SOC 2 CC7.4 · NIST RS.MA/RS.MI	Playbooks for top threats
Tabletop Exercise	ISO 5.27 · SOC 2 CC7.5 · NIST ID.IM	Tested response capability
BCP & DR Plan	ISO 5.29/5.30 · SOC 2 A1.2 · NIST RC	Recovery framework
Backup Restoration Test	ISO 8.13 · SOC 2 A1.2 · NIST RC.RP-03	Verified RTO / RPO

Phase 5 — Audit Readiness & Evidence Collection (Target: Q4 2026)

Phase 5 converts completed controls into audit-ready evidence and closes monitoring and oversight gaps.

Deliverable	Frameworks Addressed	Gap Domains Closed
Internal Audit Programme	ISO 5.35 · SOC 2 CC4.1 · NIST GV.OV	Independent assurance
Evidence Collection & Mapping	All three frameworks	SOC 2 Type II evidence package
Corrective Action Plan (CAP)	ISO 5.36 · SOC 2 CC4.2 · NIST ID.IM	Deficiency remediation tracking
SOC 2 Readiness Assessment	SOC 2 all TSC	Pre-audit gap confirmation
Auditor Engagement	SOC 2 Type II	Certification pathway

6. Gap Analysis Observations

What the Numbers Actually Mean

The gap percentages — 84%, 87%, 81% — look significant at first pass. They are the expected and honest profile of a programme completing its first formal baseline assessment. Three observations reframe the picture correctly:

The 16–19% Implemented represents controls ResolvX already had before this programme began

Okta MFA, MDM, EDR, environment separation, NDA programme, background screening. Many organisations beginning ISO 27001 start with far less. This is a strong technical foundation.

The 52–57% Partial is the most valuable data point in the entire analysis

It means ResolvX is not starting from scratch — it is formalising and evidencing controls that largely already exist. The effort required is documentation and process, not wholesale control implementation. That is a fundamentally different programme.

The 30–43% Not Done is the programme roadmap — already scoped, owned, and phased

Policy suite, IR Plan, SIEM, TPRM, and privacy programme are all Phase 3–4 deliverables. They are not surprises. They are the work ahead, and they have named owners and target dates.

The Insight Across All Three Frameworks

One pattern emerges consistently regardless of which framework is applied: ResolvX is technically ahead of where its documentation and processes suggest. The controls are largely there. The evidence, policies, and formal processes are not.

The programme's job from this point forward is to close that gap — document what exists, test what is untested, and implement what is missing. That is a programme in execution. That is the right position to be in at the end of Phase 2.

7. Document Control

Version	Date	Author	Summary
1.0	2026	Derick G. Dmello — GRC Lead	Initial gap analysis — Phase 2 baseline across ISO 27001:2022, SOC 2 TSC, and NIST CSF 2.0

Frameworks: ISO/IEC 27001:2022 | AICPA SOC 2 Trust Services Criteria | NIST Cybersecurity Framework 2.0 (February 2024)

ResolvX GRC Programme — Confidential — For Internal Distribution and Authorised External Reviewers Only — v1.0 — 2026