ResolvX

GRC Compliance & Audit Readiness Program

Stakeholder & Control Owner Register

Document Type	Version	Status	Owner	Date
Stakeholder Register	1.0	Active	GRC Lead	2026

1. Purpose

This register defines all key stakeholders in the ResolvX GRC program, their roles, responsibilities, and the specific control domains they own. Clear ownership is fundamental to a successful compliance program — without it, controls go untested, evidence goes uncollected, and audits fail.

Every control in the ResolvX control matrix maps back to an owner in this register. Owners are accountable for implementation, ongoing operation, and evidence production for their assigned controls.

2. RACI Model

The program uses a RACI model to clarify involvement across GRC activities:

Role	Definition
Responsible (R)	Does the work — implements or operates the control
Accountable (A)	Owns the outcome — signs off on the work, escalation point
Consulted (C)	Provides input or expertise before decisions are made
Informed (I)	Kept up to date on progress and outcomes

3. GRC Program Stakeholder Register

Role / Title	Name (Fictional)	Department	RACI	Primary Responsibilities
GRC Lead (Program Owner)	Derick G. Dmello	GRC & Security	A/R	Program strategy, policy development, framework mapping, audit liaison, Trust Center ownership
CISO	Jordan Mercer	GRC & Security	A	Executive sponsor, policy approvals, escalation authority, board reporting
CTO	Priya Nair	Engineering	C/I	Technology risk decisions, architecture review, security engineering alignment
VP Engineering	Marcus Webb	Engineering	R/C	Cloud security controls, DevSecOps implementation, infrastructure hardening
Head of Cloud Operations	Sam Torres	Engineering	R	AWS environment controls, patch management, logging, backup, access provisioning
Head of Product	Anya Sharma	Product	C/I	Product security requirements, privacy-by-design, feature compliance review
General Counsel / Legal	Rachel Kim	Legal	C/A	Regulatory compliance, contract security clauses, data processing agreements, GDPR/CCPA
Head of HR	David Osei	HR & Operations	R/C	Personnel security, security awareness training, background checks, offboarding
Head of Finance	Lena Vasquez	Finance	C/I	Financial data controls, SOX-adjacent requirements, vendor payment risk
Customer Success Lead	Omar Hassan	Customer Success	I	Client-facing trust communications, SOC 2 report sharing, client security questionnaires
IT Administrator	Chris Park	GRC & Security	R	Endpoint management (Jamf), M365 admin, identity administration, MFA enforcement
DevSecOps Engineer	Zara Ahmed	Engineering	R	SAST/DAST tooling, secrets scanning, vulnerability management, CI/CD security gates

4. Control Domain Ownership

The following table maps each major control domain (aligned to ISO 27001:2022 Annex A and SOC 2 TSC) to a primary owner and secondary backup. These assignments will be referenced throughout the control matrix in Phase 2.

Control Domain	ISO 27001 Ref	SOC 2 TSC	Primary Owner	Secondary Owner
Information Security Policies	A.5	CC1.1, CC1.2	GRC Lead	CISO
Organization of Information Security	A.5	CC1.3, CC1.4	GRC Lead	CISO
Human Resource Security	A.6	CC1.1, CC1.4	Head of HR	GRC Lead
Asset Management	A.5	CC6.1	Head of Cloud Ops	GRC Lead
Access Control	A.5, A.8	CC6.1, CC6.2, CC6.3	IT Administrator	Head of Cloud Ops
Cryptography	A.8	CC6.7	DevSecOps Engineer	Head of Cloud Ops
Physical & Environmental Security	A.7	CC6.4	Head of HR / Facilities	CISO
Operations Security	A.8	CC7.1, CC7.2	Head of Cloud Ops	DevSecOps Engineer
Communications Security	A.8	CC6.6, CC6.7	Head of Cloud Ops	IT Administrator
System Acquisition & Development	A.8	CC8.1	VP Engineering	DevSecOps Engineer
Supplier Relationships (TPRM)	A.5	CC9.1, CC9.2	GRC Lead	General Counsel
Incident Management	A.5, A.6	CC7.3, CC7.4, CC7.5	GRC Lead	Head of Cloud Ops
Business Continuity	A.5	A1.1, A1.2, A1.3	VP Engineering	Head of Cloud Ops
Compliance & Audit	A.5	CC4.1, CC4.2	GRC Lead	CISO
Risk Management	A.5, A.8	CC3.1, CC3.2, CC3.3	GRC Lead	CISO
Change Management	A.8	CC8.1	VP Engineering	DevSecOps Engineer
Logging & Monitoring	A.8	CC7.1, CC7.2	Head of Cloud Ops	DevSecOps Engineer

Control Domain	ISO 27001 Ref	SOC 2 TSC	Primary Owner	Secondary Owner
Vulnerability Management	A.8	CC7.1	DevSecOps Engineer	Head of Cloud Ops
Data Privacy & Protection	A.5, A.8	P1–P8 (Privacy)	General Counsel	GRC Lead
Security Awareness & Training	A.6	CC1.4, CC2.2	Head of HR	GRC Lead

5. Escalation Path

When a control gap, risk event, or compliance issue is identified, the following escalation path applies:

Level	Trigger	Escalate To	Timeframe
Level 1 — Operational	Control deficiency identified during testing	GRC Lead	Within 5 business days
Level 2 — Program	High-severity gap or failed audit finding	CISO	Within 48 hours
Level 3 — Executive	Critical risk, breach, or regulatory notification required	CTO / CEO / Legal	Immediately
Level 4 — Board	Material incident or significant compliance failure	Board of Directors	Within 72 hours of Level 3

6. Document Control

Version	Date	Author	Change Summary
1.0	2026	Derick G. Dmello	Initial stakeholder and control owner register — Phase 1 baseline