ResolvX

GRC Compliance & Audit Readiness Program

Objectives, Scope & Goals

Document Type	Version	Status	Owner	Date
Program Charter	1.0	Active	GRC Lead	2026

1. Executive Summary

ResolvX is a cloud-native SaaS fintech company providing AI-powered financial resolution services to enterprise clients. As the business scales and onboards regulated financial institutions, a formal, defensible security compliance posture is a commercial and regulatory necessity.

This document establishes the formal charter for ResolvX's internal GRC program. It defines the program's purpose, boundaries, target frameworks, and measurable goals that will guide all compliance and risk management activities through to audit readiness and Trust Center launch.

2. Program Objectives

The ResolvX GRC program is designed to achieve the following core objectives:

2.1 Establish a Risk-Aware Culture

- Implement a structured, repeatable risk management process aligned to ISO 31000 and NIST RMF
- Ensure all business units understand their risk responsibilities through defined control ownership
- Maintain a live risk register that reflects the current threat landscape

2.2 Achieve Compliance Certification

- Attain SOC 2 Type II certification within 18 months of program initiation
- Align controls with ISO 27001:2022 Annex A in preparation for future certification
- Ensure PCI-DSS v4.0 compliance for all cardholder data environments

2.3 Build Audit-Ready Evidence Practices

- Establish a structured evidence library supporting all major framework requirements
- Conduct quarterly internal audits to validate control effectiveness
- Maintain continuous compliance monitoring through a compliance dashboard

2.4 Launch a Public Trust Center

- Publish a customer-facing Trust Center documenting security posture, certifications, and privacy practices
- Provide real-time or near-real-time compliance status visibility to enterprise prospects and clients

3. Scope

3.1 In-Scope

The following assets, systems, and processes are within the scope of this GRC program:

Scope Item	Description	Applicable Frameworks
AWS Cloud Infrastructure	3 environments: Production, Staging, Dev (us-east-1)	ISO 27001, SOC 2, NIST CSF
SaaS Application	ResolvX core platform — customer-facing dispute resolution app	SOC 2, PCI-DSS
Corporate IT	Laptops, M365, SaaS tools (Slack, Notion, GitHub)	ISO 27001, NIST CSF
Data Processing	PII, financial transaction records, client data	PCI-DSS, SOC 2, ISO 27001
Third-Party Vendors	AWS, Stripe, SendGrid, Okta, GitHub	ISO 27001, SOC 2
Personnel	All full-time employees and contractors with system access	ISO 27001, SOC 2

3.2 Out of Scope

- Physical office security (leased facility — landlord responsibility)
- Personal devices not enrolled in MDM
- Acquired subsidiaries pending integration assessment

4. Target Compliance Frameworks

Framework	Version	Purpose	Target Date
SOC 2 Type II	AICPA TSC 2017	Primary certification — enterprise client requirement	Q4 2026
ISO 27001	2022 Edition	ISMS baseline — controls and risk management	Q2 2027
NIST CSF	2.0 (2024)	Internal security program structure and maturity	Ongoing
PCI-DSS	v4.0	Payment card data protection	Q3 2026

5. Goals & Success Metrics

Goal	Metric	Target
Complete baseline risk assessment	Risk register with 15+ identified risks, scored and mitigated	Phase 2
Map all controls to frameworks	90%+ control coverage across SOC 2 TSC and ISO 27001 Annex A	Phase 2
Develop full policy library	8+ policies authored, approved, and version-controlled	Phase 3
Complete vendor assessments	100% of Tier 1 vendors assessed and scored	Phase 3
IR plan tested	Tabletop simulation completed with documented findings	Phase 4
Internal audit completed	Audit report with CAP issued and tracked	Phase 5
Trust Center live	Public trust page with certs, controls, and privacy summary	Phase 6

6. Roles & Responsibilities

Role	Responsibility
GRC Lead (Program Owner)	Owns program strategy, roadmap, policy development, audit liaison
CISO / VP Engineering	Executive sponsor — approves policies, escalation point
IT/Cloud Operations	Control implementation, evidence collection, infrastructure security
Legal & Privacy	Regulatory compliance, data protection, contract reviews
HR	Security awareness, personnel security controls
Department Heads	Control owners within their business units

7. Document Control

Version	Date	Author	Change Summary
1.0	2026	Derick G. Dmello	Initial program charter — baseline scope and objectives