ResolvX

GRC Compliance & Audit Readiness Program

Program Roadmap | v1.0

Document Type	Version	Status	Owner	Horizon
Program Roadmap	1.0	Active	GRC Lead	2026 – 2027

Roadmap Overview

The ResolvX GRC program is structured across six sequential phases. Each phase builds on the previous, creating a compounding foundation that culminates in a mature, audit-ready compliance program with a public Trust Center. Phases may partially overlap where dependencies allow.

Phase	Name	Timeline	Key Output	Status
Phase 1	Foundation	Month 1–2	Charter, scope, company profile, stakeholder register	🟡 In Progress
Phase 2	Risk & Controls	Month 2–4	Risk register, framework control matrix, gap analysis report	☐ Planned
Phase 3	Policies & Vendor Risk	Month 4–6	Policy library (8+ docs), vendor assessments, TPRM register	☐ Planned
Phase 4	Incident Response	Month 6–8	IR plan, runbooks, tabletop simulation report	☐ Planned
Phase 5	Audit Readiness	Month 8–11	Internal audit report, evidence library, corrective action plan	☐ Planned
Phase 6	Trust Center	Month 11–14	Public trust center, compliance dashboard, certification showcase	☐ Planned

Phase 1 — Foundation

Objective

Establish the structural foundation for the entire GRC program. Define what ResolvX is, what it needs to protect, who owns what, and how the program will operate.

Deliverables

- Objectives, Scope & Goals document
- Program Roadmap
- Company profile and asset inventory
- Stakeholder and control owner register
- GitHub repository structure initialized

Success Criteria

- Program formally scoped with executive alignment
- All foundational documents reviewed and version-controlled
- Repo structure established and ready for Phase 2 content

Phase 2 — Risk & Controls

Objective

Build the risk management foundation. Identify, score, and prioritize ResolvX's key security risks. Map existing and planned controls to ISO 27001, SOC 2, and NIST CSF frameworks. Identify gaps.

Deliverables

- Risk register (Excel) — 15+ risks, likelihood/impact scoring, heat map, mitigation owners
- Risk methodology document
- ISO 27001 Annex A control matrix — full 93-control mapping with status and owners
- SOC 2 TSC criteria mapping (CC1–CC9)
- NIST CSF 2.0 function-level mapping
- Gap analysis report (consolidated findings across all frameworks)

Success Criteria

- All identified risks scored and assigned to owners
- Control coverage mapped at 80%+ across SOC 2 and ISO 27001
- Gap analysis report approved and gap remediation prioritized

Phase 3 — Policies & Vendor Risk

Objective

Translate framework requirements into actionable policies. Assess the security posture of key third-party vendors who handle ResolvX data or infrastructure.

Deliverables

- Information Security Policy
- Access Control Policy
- Incident Response Policy
- Data Classification Policy
- Vendor Management Policy
- Acceptable Use Policy
- Vendor assessment questionnaire template (25+ questions, scored)
- Vendor risk register with Tier 1 assessments completed (AWS, Stripe, Okta)
- Vendor risk scorecard and assessment reports

Success Criteria

- All policies reviewed, approved, and version-controlled
- 100% of Tier 1 vendors assessed with risk rating assigned

Phase 4 — Incident Response

Objective

Design, document, and test ResolvX's incident response capability. Align to ISO 27035 and NIST SP 800-61 standards.

Deliverables

- Incident Response Plan — full lifecycle (Prepare, Detect, Contain, Eradicate, Recover, Lessons Learned)
- Runbooks for: Phishing, Ransomware, Data Breach
- Tabletop simulation scenario and facilitation guide
- Post-simulation report with findings and remediation actions
- Incident log template

Success Criteria

- IR plan covers all NIST IR lifecycle phases
- At least one tabletop simulation completed and documented
- All critical IR roles assigned to named owners

Phase 5 — Audit Readiness

Objective

Perform a structured internal audit of all controls implemented across Phases 1–4. Collect evidence, identify non-conformities, and produce a corrective action plan. Simulate the experience of a SOC 2 Type II pre-audit.

Deliverables

- Internal audit checklist (Control, Evidence, Finding, Severity, Action Plan)
- Evidence library — organized by framework, with screenshots and documentation
- Internal audit report — findings, ratings, and lessons learned
- Corrective Action Plan (CAP) — tracked with owners and target dates
- SOC 2 Type II readiness assessment report

Success Criteria

- All in-scope controls tested with evidence collected or gaps documented
- Audit report issued with severity-classified findings
- CAP addresses all High and Critical findings

Phase 6 — Trust Center

Objective

Synthesize the entire program into a public-facing Trust Center that demonstrates ResolvX's security and compliance posture to enterprise prospects, customers, and auditors.

Deliverables

- Compliance dashboard (Excel/Power BI) — control coverage, risk trends, KRIs/KPIs
- Trust Center overview page
- Security overview document — controls, architecture, and security practices
- Privacy and data handling overview
- Certifications and audit reports index
- Subprocessor and vendor list
- Interactive trust center prototype (HTML/web artifact)

Success Criteria

- Trust center accurately reflects program maturity at program completion
- All major certification targets and compliance milestones documented
- Portfolio-ready showcase demonstrating end-to-end program ownership

Key Milestones Summary

Milestone	Phase	Target
Program charter finalized	1	Month 1
Risk register complete	2	Month 3
Full control matrix mapped	2	Month 4
Policy library complete	3	Month 6
Vendor assessments complete	3	Month 6
IR plan tested	4	Month 8
Internal audit report issued	5	Month 10
SOC 2 readiness report complete	5	Month 11
Trust Center launched	6	Month 14