INFORMATION SECURITY

RISK SUMMARY REPORT

ResolvX - GRC Compliance & Audit Readiness Programme

Phase 2: Risk & Controls | Version 1.0 | 2026

Classification	Owner	Methodology	Review Cycle
Confidential	GRC Lead — D. Dmello	NIST 800-30 + FAIR	Quarterly

Executive Summary

ResolvX has completed its inaugural formal information security risk assessment as part of Phase 2 of the GRC Compliance & Audit Readiness Programme. This report presents findings to organisational leadership, providing a clear view of ResolvX's current risk posture, the financial exposure associated with top risks, and the remediation priorities required to achieve target compliance certifications and protect client trust.

25 risks were identified and assessed across five categories: Cyber Threat, Cloud & Infrastructure, Vendor & Third-Party, Compliance & Regulatory, and Human & Operational. The assessment applied the NIST SP 800-30 Rev. 1 methodology for qualitative scoring and the FAIR model for financial quantification of high and critical risks.

Key Findings at a Glance

Total risks assessed	25 across 5 categories
Critical risks (residual)	0 — all critical inherent risks reduced through controls
High risks (residual)	**8 requiring treatment plans within 30 days**
Moderate risks (residual)	**11 requiring treatment plans within 90 days**
Low / Very Low (residual)	**6 — accepted or monitored**
Total FAIR ALE exposure	$2.3M – $9.6M annualised across quantified risks
Top single risk ALE	RSK-001 Ransomware — $350K – $1.2M per year
Risks with treatment plans	25 / 25 — all risks have documented treatment decisions
Overall risk trajectory	**Improving — controls reducing residual scores across all categories**

Assessment Note

Figures represent residual risk after accounting for current controls. The shift from 8 Critical inherent risks to 0 Critical residual risks demonstrates that existing controls — Okta MFA, GuardDuty, EDR, multi-AZ, and GitHub branch protection — are delivering meaningful risk reduction.

1. Risk Posture Overview

1.1 Inherent vs Residual Risk Distribution

The following table shows how ResolvX's current controls shift risk levels from inherent (pre-control) to residual (post-control). This movement is the primary metric of control programme effectiveness.

Risk Level	Score	Inherent	Residual	Delta
🔴 **Critical**	20–25	8	0	**-8**
🔴 **High**	12–19	10	8	**-2**
🟠 **Moderate**	7–11	5	11	**+6**
🟡 **Low**	4–6	2	5	**+3**
🟢 **Very Low**	1–3	0	1	**+1**

The moderate increase in the Moderate bucket reflects correct risk accounting - risks that were Critical or High inherently become Moderate after control credit. This is the expected profile of a programme with foundational controls in place but not yet at full maturity.

1.2 Risk Distribution by Category

Category	Risks	Highest Residual	Primary Driver
Cyber Threat	5	**High**	Ransomware, phishing, API exploitation
Cloud & Infrastructure	5	**High**	IAM over-privilege, S3 misconfiguration
Vendor & Third-Party	5	**Moderate**	No formal TPRM programme
Compliance & Regulatory	5	**High**	SOC 2 Type II not yet certified
Human & Operational	5	**Moderate**	Offboarding gaps, BCP absence

2. Top 8 High Residual Risks

These risks require formal treatment plans and active remediation. Each is assigned a named control owner and target completion date.

RSK-001 — Ransomware Attack

Residual Score	**12 (L3 × I4)**
Threat Source	Organised cybercriminal / RaaS
Core Vulnerability	No immutable backup vault; no tabletop exercise
FAIR ALE	$350,000 – $1,200,000 / year
Control Owner	Head of Cloud Ops
Treatment	AWS Backup vault lock; immutable S3 backups; ransomware tabletop
Target Date	Q2 2026

RSK-003 — API Vulnerability Exploitation

Residual Score	**10 (L2 × I5)**
Threat Source	External attacker — opportunistic/targeted
Core Vulnerability	Quarterly scanning insufficient; no pen test completed
FAIR ALE	$280,000 – $950,000 / year
Control Owner	DevSecOps Engineer
Treatment	Weekly scanning; 30-day CVE SLA; annual penetration test
Target Date	Q1 2026

RSK-004 — Insider Threat / Data Exfiltration

Residual Score	**8 (L2 × I4)**
Threat Source	Malicious or negligent insider
Core Vulnerability	No DLP tooling; no UEBA; access reviews not quarterly
FAIR ALE	$150,000 – $600,000 / year

Control Owner	GRC Lead
Treatment	Implement DLP; deploy UEBA alerting; enforce quarterly access reviews
Target Date	Q3 2026

RSK-005 — Software Supply Chain Attack

Residual Score	**12 (L3 × I4)**
Threat Source	Nation-state / sophisticated threat actor
Core Vulnerability	No SBOM; SAST not fully deployed; no vetting process
FAIR ALE	$200,000 – $800,000 / year
Control Owner	DevSecOps Engineer
Treatment	SBOM generation; code signing; full SAST/SCA in CI/CD
Target Date	Q2 2026

RSK-006 — AWS S3 Misconfiguration

Residual Score	**10 (L2 × I5)**
Threat Source	Internal — configuration error
Core Vulnerability	IaC not fully enforced; no monthly CSPM review
FAIR ALE	$180,000 – $750,000 / year
Control Owner	Head of Cloud Ops
Treatment	Security Hub CIS checks; IaC policy guardrails; monthly CSPM review
Target Date	Q1 2026

RSK-008 — IAM Over-Privilege

Residual Score	**12 (L3 × I4)**
Threat Source	External attacker exploiting over-privileged roles
Core Vulnerability	No formal PAM programme; IAM Access Analyzer not deployed
FAIR ALE	$130,000 – $520,000 / year
Control Owner	Head of Cloud Ops

Treatment	Full IAM access review; deploy IAM Access Analyzer; implement SCPs
Target Date	Q2 2026

RSK-016 — SOC 2 Type II Failure

Residual Score	**8 (L2 × I4)**
Threat Source	Internal — programme execution risk
Core Vulnerability	Audit engagement not initiated; policies not published
FAIR ALE	$500,000+ in deferred ARR pipeline
Control Owner	GRC Lead
Treatment	Execute GRC roadmap; engage auditor by Q3 2026; complete Phase 3 policies
Target Date	Q3 2026

RSK-017 — GDPR Violation

Residual Score	**8 (L2 × I4)**
Threat Source	Internal process gap / DSR failure
Core Vulnerability	No ROPA; no DSR process; GDPR data mapping incomplete
FAIR ALE	$200,000 – $2,000,000 / year
Control Owner	General Counsel
Treatment	GDPR data mapping; DSR process; complete ROPA
Target Date	Q2 2026

3. FAIR Quantitative Risk Analysis

FAIR analysis was applied to all risks scoring 12 or above on the residual 5×5 matrix. The following table presents the full financial exposure picture across all quantified risks.

3.1 Annualised Loss Expectancy Summary

ID	Risk	Level	ALE Low	ALE High	ALE Mid	Mid ALE
RSK-001	Ransomware attack	•	$350K	$1.2M	$775K	
RSK-002	Phishing / credential theft	•	$95K	$420K	$258K	
RSK-003	API vulnerability exploitation	•	$280K	$950K	$615K	
RSK-004	Insider threat / exfiltration	•	$150K	$600K	$375K	
RSK-005	Supply chain attack	•	$200K	$800K	$500K	
RSK-006	AWS S3 misconfiguration	•	$180K	$750K	$465K	
RSK-008	IAM over-privilege	•	$130K	$520K	$325K	
RSK-012	Stripe integration breach	•	$250K	$850K	$550K	
RSK-016	SOC 2 certification failure	•	$500K	$1.5M	$1.0M	
RSK-017	GDPR violation	•	$200K	$2.0M	$1.1M	
TOTAL			**$2.3M**	**$9.6M**	**$6.0M**	

Interpretation Note

ALE figures represent annualised probable loss ranges based on FAIR methodology. They are probabilistic estimates informed by threat frequency, control effectiveness, and industry loss data — not predictions. Use them to prioritise investment decisions, not as precise forecasts. Total FAIR ALE mid-point ($6.0M) represents the annualised risk if all quantified events were to occur proportionally.

3.2 FAIR Loss Decomposition — Top 3 Risks

RSK-001 Ransomware — $775K Mid ALE

TEF (Threat Event Frequency)	2.0 events/year — industry average for fintech sector
Vulnerability (control gap)	35% — GuardDuty + EDR reduce but do not eliminate exposure
LEF (Loss Event Frequency)	0.7 events/year
Primary Loss	$180K — IR costs, recovery operations, breach notification
Secondary Loss	$930K — regulatory fines, legal, reputational, client churn
Loss Magnitude per Event	$1,110K

RSK-017 GDPR Violation — $1,100K Mid ALE

TEF	1.5 incidents/year — GDPR enforcement active in financial services
Vulnerability	45% — no ROPA, no DSR process = elevated exposure
LEF	0.675 incidents/year
Primary Loss	$120K — legal response, notification, remediation
Secondary Loss	$1,508K — fine up to 4% global revenue + litigation
Loss Magnitude per Event	$1,628K

RSK-016 SOC 2 Failure — $1,000K Mid ALE

Commercial Risk Profile

RSK-016 is unique — loss is primarily commercial, not incident-driven. Each quarter of delay costs an estimated $125K in deferred enterprise ARR. Full certification failure would cost $500K–$1.5M in lost pipeline within 12 months. Treatment is programme execution, not a technical control.

4. Risk Treatment Progress

4.1 Treatment Decision Summary

Treatment	Count	%	Rationale	Risk Level
Mitigate	21	84%	Primary response — implement or strengthen controls	High/Med
Transfer / Mitigate	1	4%	RSK-011 AWS concentration — cyber insurance + DR	High
Accept / Mitigate	1	4%	RSK-020 SLA breach — buffer SLAs + monitor	Moderate
Accept	2	8%	RSK-023 key person (documentation); RSK-015 SendGrid (low)	Low

4.2 Treatment Timeline

Horizon	Risk IDs	Focus Area
Q1 2026 — Immediate	RSK-003, 006, 009, 015	API scanning · S3 posture · Secrets management · DMARC
Q2 2026 — 30–60 days	RSK-001, 002, 005, 008, 012, 013, 017	Ransomware controls · FIDO2 MFA · Supply chain · IAM · GDPR
Q3 2026 — 60–90 days	RSK-004, 016, 018, 019	DLP/UEBA · SOC 2 audit engagement · PCI-DSS · CCPA
Q4 2026 — Ongoing	RSK-007, 011, 020, 023	DR strategy · Vendor concentration · SLA management · Key person

5. Risk Programme Observations

What Is Working

The foundational security controls deployed at ResolvX — Okta SSO with MFA, AWS GuardDuty, EDR on all endpoints, GitHub branch protection, multi-AZ architecture, and Jamf MDM — are collectively reducing inherent risk scores meaningfully. No risks remain at Critical residual level. This is a strong foundation for a company at this stage of the GRC programme.

Where the Programme Must Focus

Three themes dominate the residual risk profile:

Theme 1 — Detection & Response Gap

The absence of a SIEM, formalised IR Plan, and comprehensive alerting means that even well-protected systems have limited detection capability. An attacker who bypasses perimeter controls could operate undetected for extended periods. SIEM deployment and IR Plan development (Phase 4) are the highest-leverage investments on the roadmap.

Theme 2 — Cloud Posture Discipline

AWS misconfiguration (RSK-006), IAM over-privilege (RSK-008), and secrets management gaps (RSK-009) stem from the same root cause: fast-moving engineering without fully mature DevSecOps controls. IaC enforcement and a CSPM programme address all three simultaneously.

Theme 3 — Compliance Programme Execution

RSK-016 (SOC 2 failure) carries the highest single commercial risk in the portfolio. It is a programme execution risk, not a technical one. Every week of delay on policy development (Phase 3) and auditor engagement reduces the probability of Q4 2026 certification. This risk is owned by the GRC Lead and CISO.

Risk Appetite Alignment

ResolvX's stated risk appetite — Low for cybersecurity, Very Low for compliance — is consistent with the residual risk profile. All 8 High residual risks have documented treatment plans with named owners and target dates. No risks sit unattended above the accepted tolerance threshold. The programme is operating within its own risk framework.

6. Recommended Board-Level Actions

1

Approve security budget for SIEM and CSPM tooling — Q1 2026

The detection gap is the most significant unmitigated risk cluster. AWS Security Hub + a SIEM solution (estimated $40K–$80K annually) closes RSK-010, reduces RSK-007 (partial), and addresses the NIST CSF DE function gaps identified in the framework mapping. ROI is direct — current FAIR exposure in the DE gap cluster exceeds $1.5M ALE mid.

2

Formally engage a SOC 2 auditor by Q3 2026

RSK-016 requires a firm external commitment. Engaging an auditor creates a fixed deadline that drives Phase 3–5 execution and signals to enterprise clients that certification is on a defined timeline. Recommended audit firms for SaaS fintech: A-LIGN, Schellman, Drata/Vanta-partnered practices.

3

Initiate GDPR data mapping and DSR programme — Q2 2026

GDPR carries the highest potential ALE in the portfolio ($200K–$2M). ResolvX processes EU financial data, making this exposure material. A focused 6-week sprint — ROPA, DSR workflow, DPA review — would reduce RSK-017 residual score from 8 to 4 and demonstrate regulatory maturity to European financial institution clients.

7. Document Control

Version	Date	Author	Summary
1.0	2026	Derick G. Dmello — GRC Lead	Initial report — Phase 2 baseline assessment

Methodology: NIST SP 800-30 Rev. 1 (Qualitative Scoring) | FAIR (Quantitative ALE) | ISO/IEC 27001:2022 (Control Reference)

ResolvX GRC Programme — Confidential — For Internal Distribution and Authorised External Reviewers Only