

ResolvX

GRC Compliance & Audit Readiness Program

Risk Assessment Methodology

Document Type	Version	Status	Owner	Standard
Risk Methodology	1.0	Active	GRC Lead	NIST 800-30 ISO 27001 FAIR

1. Purpose

This document defines how ResolvX identifies, analyzes, evaluates, and treats information security risks. It establishes the rules of engagement before any risk is scored, this methodology defines what the scores mean, how they are derived, and what actions follow.

A consistent, repeatable methodology ensures that risk assessments remain comparable over time, defensible to auditors, and actionable for the business. This document is a mandatory reference for all GRC, security, and audit activities at ResolvX.

2. Governing Standards

Standard	Role in This Methodology
NIST SP 800-30 Rev. 1	Core risk assessment process : threat identification, likelihood and impact scales, risk determination
ISO/IEC 27001:2022	ISMS risk management requirements : Clause 6.1.2 (risk assessment), Clause 6.1.3 (risk treatment)
ISO 31000:2018	Risk management principles, framework, and process
FAIR (Factor Analysis of Information Risk)	Quantitative model for top-tier risks : produces probable financial loss ranges in dollar terms

3. Risk Assessment Process

ResolvX follows the four-step risk assessment lifecycle defined in NIST SP 800-30 Rev. 1:

Step	Phase	Key Activities
1	Prepare	Define scope, identify assets and threat sources, assign risk owners, establish assessment approach
2	Conduct	Identify threat events and vulnerabilities, determine likelihood and impact scores, calculate inherent and residual risk
3	Communicate	Produce risk register and executive summary, brief stakeholders, escalate High and Critical risks
4	Maintain	Quarterly register review, update scores on material changes, track treatment plan progress

4. Model 1 — Qualitative: 5x5 Risk Matrix

The 5x5 qualitative model is applied to all risks in the ResolvX risk register. It produces an inherent risk score (before controls) and a residual risk score (after controls), enabling comparison across the full risk portfolio.

4.1 Likelihood Scale

Source: NIST SP 800-30 Rev. 1, Appendix G — tailored for ResolvX context.

Score	Level	Adversarial (Threat Actor)	Non-Adversarial (Error / Nature)
5	Very High	Adversary is almost certain to initiate the threat event	Occurs more than 100 times per year
4	High	Adversary is highly likely to initiate the threat event	Occurs between 10 - 100 times per year
3	Moderate	Adversary is somewhat likely to initiate the threat event	Occurs between 1 - 10 times per year
2	Low	Adversary is unlikely to initiate the threat event	Occurs less than once per year
1	Very Low	Adversary is highly unlikely to initiate the threat event	Occurs less than once every 10 years

4.2 Impact Scale

Source: NIST SP 800-30 Rev. 1, Appendix H — tailored for ResolvX operations.

Score	Level	Definition	ResolvX Examples
5	Very High	Catastrophic — existential threat to operations, regulatory standing, or market position	Mass PII breach, complete platform outage >24hrs, loss of SOC 2 certification

Score	Level	Definition	ResolvX Examples
4	High	Severe — major disruption to operations, finances, or client relationships	Significant data loss, regulatory fine >\$500K, major client churn, reputational crisis
3	Moderate	Significant — notable disruption but recoverable within normal operations	Partial data exposure, service degradation, failed audit finding, SLA breach
2	Low	Minor — limited operational or reputational impact	Single account compromise, minor SLA breach, internal policy violation with no data impact
1	Very Low	Negligible — minimal impact, fully and quickly recoverable	Near-miss event with no data exposure, minor process deviation

4.3 Risk Score Matrix

Risk Score = Likelihood × Impact. The matrix below shows all possible score combinations and their corresponding risk levels.

L \ I	Impact 1	Impact 2	Impact 3	Impact 4	Impact 5
Likelihood 5	5 — Low	10 — Moderate	15 — High	20 — Critical	25 — Critical
Likelihood 4	4 — Very Low	8 — Low	12 — Moderate	16 — High	20 — Critical
Likelihood 3	3 — Very Low	6 — Low	9 — Low	12 — Moderate	15 — High
Likelihood 2	2 — Very Low	4 — Very Low	6 — Low	8 — Low	10 — Moderate
Likelihood 1	1 — Very Low	2 — Very Low	3 — Very Low	4 — Very Low	5 — Low

4.4 Risk Level Thresholds & Response

Score	Risk Level	Required Response	Timeframe
20–25	CRITICAL	Immediate escalation to CISO. Emergency treatment plan.	Within 72 hours
12–19	HIGH	Escalate to GRC Lead. Formal treatment plan required.	Within 30 days
7–11	MODERATE	Assign to control owner. Treatment plan documented.	Within 90 days
4–6	LOW	Monitor quarterly. Accept or treat at GRC Lead discretion.	Next quarterly review
1–3	VERY LOW	Accept risk. Document rationale in register.	Annual review

5. Model 2 — Quantitative: FAIR Analysis

FAIR (Factor Analysis of Information Risk) is applied to all risks scoring 12 or above (High or Critical) in the 5x5 qualitative model. FAIR produces an Annualized Loss Expectancy (ALE) - a probable financial loss range expressed in dollars - that enables executive-level risk prioritization and informs cyber insurance decisions.

5.1 FAIR Model Structure

FAIR decomposes risk into two primary factors: Loss Event Frequency and Loss Magnitude.

FAIR Component	Sub-Components	Definition
Risk	Loss Event Frequency × Loss Magnitude	The probable frequency and magnitude of future loss
Loss Event Frequency (LEF)	TEF × Vulnerability	How often a loss-generating event actually occurs per year
Threat Event Frequency (TEF)	Contact Frequency × Probability of Action	How often a threat agent acts against the asset
Vulnerability	Control Strength vs. Threat Capability	Probability a threat event results in an actual loss (0–100%)
Loss Magnitude (LM)	Primary Loss + Secondary Loss	Total financial impact when a loss event occurs
Primary Loss	Productivity, Response, Replacement	Direct costs from the loss event itself
Secondary Loss	Fines, Legal, Reputational, Client Churn	Downstream costs triggered by the loss event

5.2 ResolvX Loss Categories

Loss Category	Type	ResolvX Examples	Estimation Basis
Productivity Loss	Primary	Engineering hours diverted to incident response, downtime	Fully loaded hourly rate × hours lost
Response Costs	Primary	Forensics, legal counsel, breach notification, PR	Vendor contracts + external counsel rates
Replacement Costs	Primary	Data recovery, system rebuild, hardware/software	Cloud spend + internal labor costs
Regulatory Fines	Secondary	NYDFS, CCPA (\$100–\$750/record), GDPR (up to 4% global revenue)	Published regulatory fine schedules
Legal Liability	Secondary	Client lawsuits, contractual SLA penalties, indemnification	Contract terms + litigation cost estimates

Loss Category	Type	ResolvX Examples	Estimation Basis
Reputational Loss	Secondary	Client churn, delayed sales cycles, reduced valuation	ARR × estimated churn rate × deal velocity impact

5.3 FAIR Output Format

For each High/Critical risk, FAIR analysis produces the following output documented in the risk register:

FAIR Output Field	Description	Example
TEF (per year)	How often the threat agent acts	Ransomware group: 2× per year industry avg.
Vulnerability (%)	Probability of successful loss event	Current controls = 65% effective → 35% vuln.
LEF (per year)	Expected loss events per year	$2 \times 0.35 = 0.7$ events/year
Primary Loss (\$)	Direct financial impact	\$180,000 (IR + recovery + notification)
Secondary Loss (\$)	Downstream financial impact	\$320,000 (fines + legal + churn)
Loss Magnitude (\$)	Total per-event impact	\$500,000
ALE (Annualized)	Expected annual loss	$0.7 \times \$500,000 = \$350,000/\text{year}$
ALE Range	Min–Max loss estimate	\$175,000 – \$1,200,000/year

6. Risk Appetite & Tolerance

Risk Category	Appetite	Rationale
Cybersecurity	Low	ResolvX cannot tolerate risks that could result in client data exposure or platform unavailability
Compliance & Regulatory	Very Low	Zero tolerance — regulatory violations can revoke our right to operate as a service organization
Vendor / Third-Party	Moderate	Acceptable where compensating controls exist and vendor SOC 2 reports are current
Operational	Moderate	Acceptable for non-critical processes with defined and tested recovery procedures
Reputational	Very Low	Trust is ResolvX's core value proposition — reputational risk is treated as critical

7. Risk Treatment Options

Treatment	Definition	Application at ResolvX
Mitigate	Implement or enhance controls to reduce likelihood or impact	Primary response for all High and Critical risks
Transfer	Shift financial exposure to a third party — cyber insurance, contractual terms	Applied where financial loss magnitude is the primary concern
Accept	Formally acknowledge and accept the risk as-is	Low/Very Low risks, or where treatment cost exceeds expected loss
Avoid	Eliminate the activity, system, or asset generating the risk	Applied where risk cannot be reduced to acceptable tolerance levels

8. Risk Register Data Dictionary

Every risk entry in the ResolvX risk register captures the following fields. This dictionary ensures consistency across all assessors and audit cycles.

Field	Description
Risk ID	Unique identifier — format: RSK-XXX (e.g., RSK-001)
Category	Cyber / Cloud & Infrastructure / Vendor & Third-Party / Compliance & Regulatory
Risk Description	Clear, unambiguous statement of the risk scenario (threat + asset + consequence)
Threat Source	The agent initiating the risk — external actor, insider, system failure, natural event
Affected Assets	Specific systems, data classifications, or processes impacted
Inherent Likelihood (1–5)	Likelihood score before any controls are applied
Inherent Impact (1–5)	Impact score before any controls are applied
Inherent Risk Score	Inherent Likelihood × Inherent Impact
Current Controls	Controls currently in place that reduce likelihood or impact
Control Effectiveness	Assessment of how well current controls reduce the risk (Strong/Moderate/Weak)
Residual Likelihood (1–5)	Likelihood score after current controls are considered
Residual Impact (1–5)	Impact score after current controls are considered
Residual Risk Score	Residual Likelihood × Residual Impact — the live risk level
Risk Level	Very Low / Low / Moderate / High / Critical — derived from residual score

Field	Description
FAIR ALE (\$)	Annualized Loss Expectancy for High and Critical risks
Treatment Decision	Mitigate / Transfer / Accept / Avoid
Treatment Actions	Specific, actionable remediation steps with owners
Control Owner	Named individual responsible for treatment and evidence
Target Completion Date	Deadline for treatment action completion
Status	Open / In Progress / Closed / Accepted
ISO 27001:2022 Ref	Relevant Annex A control domain(s)
SOC 2 TSC Ref	Relevant Trust Services Criteria reference(s)
Last Reviewed	Date of last risk score review

9. Review & Maintenance Cycle

Trigger	Required Action	Owner
Quarterly scheduled review	Full register review — update all scores, treatment status, control effectiveness	GRC Lead
Material change event	New system, vendor, regulation, or product feature added — assess new risks within 30 days	GRC Lead + Control Owner
Post-security incident	Re-assess all risks related to the incident — update scores and treatment plans	GRC Lead + CISO
Pre-audit engagement	Full risk register refresh — ensure all scores current and treatment plans documented	GRC Lead
Annual assessment	Comprehensive reassessment — review risk appetite, methodology currency, and threat landscape	GRC Lead + CISO

10. Document Control

Version	Date	Author	Change Summary
1.0	2026	Derick G. Dmello	Initial risk assessment methodology — Phase 2 baseline