

RISK REGISTER

Information Security and Operational Risk Register

Control Reference	BIZOPS-11
Document Version	1.0
Effective Date	June 1, 2026
Next Review	June 1, 2027
Classification	Confidential – Internal & Customer Use
Maintained by	Altnetix LLC Security & Compliance Team
Contact	compliance@altnetix.com

Risk Register Overview

This Risk Register documents identified risks to the confidentiality, integrity, and availability of Altnetix LLC's information systems and PHI. Risks are assessed quarterly and following material changes. Scoring: Likelihood 1-5 × Impact 1-5 = Risk Score. Residual Risk reflects score after controls applied.

Current Risk Register

Risk ID	Risk Description	Likelihood	Impact	Score	Controls in Place	Residual	Owner	Status
R-001	PHI breach via stolen	3	5	15	MFA, RBAC	6	Security	Mitigated
R-002	Ransomware / malware	2	5	10	EDR, immutable	4	DevOps	Mitigated
R-003	SQL injection /	2	4	8	Input sanitization, WAF	2	Engineering	Mitigated
R-004	Third-party vendor PHU	2	4	8	BAA, vendor risk	4	Security	Monitored
R-005	Insider threat / un	2	4	8	RBAC, audit	4	HR/Security	Mitigated
R-006	Azure region	1	5	5	Geo-redundant	2	DevOps	Mitigated
R-007	Expired TLS	2	3	6	Cert monitoring	1	DevOps	Mitigated
R-008	Phishing / social	3	3	9	Security awareness	4	HR/Security	Monitored
R-009	Unpatched dependencies	3	3	9	Dependabot, monthly	4	Engineering	Monitored
R-010	Regulatory changes	2	3	6	Compliance	3	Security	Monitored
R-011	Business continuity	3	4	12	Documentat ion, cross	6	CEO	Open
R-012	Lack of cyber person dependency coverage	4	4	16	Cyber insurance pr review plan in progress	8	Legal	In Progress

Risk Treatment Summary

Risk Distribution

- Critical (20-25): 0 risks
- High (13-19): 1 risk (R-012, pending cyber insurance)
- Moderate (6-12): 5 risks
- Low (1-5): 6 risks

Overall security posture is MODERATE with active mitigation programs. Priority actions: obtain cyber insurance (R-012), implement key-person cross-training (R-011).