RISK REGISTER

Security Risk Assessment Deliverable

Client:	[SAMPLE COMPANY]
Assessment Date:	December 2024
Assessor:	Careful Security
Classification:	Confidential

Total Risks	Critical	High	Medium	Low
47	8	15	18	6

SAMPLE DOCUMENT - All client information anonymized

DETAILED RISK REGISTER

Each risk is scored using the CVSS (Common Vulnerability Scoring System) methodology, considering likelihood, impact, and exploitability factors.

ID	Risk Description	Category	Score	Priority
R-001	No MFA enabled on administrator accounts	Access Control	9.5	CRITICAL
R-002	Production servers running unpatched software (>90 days)	Vulnerability	9.1	CRITICAL
R-003	AWS S3 buckets publicly accessible	Cloud Security	9.1	CRITICAL
R-004	No encryption at rest for customer PII	Data Protection	8.8	CRITICAL
R-005	Shared service accounts across teams	Access Control	8.5	CRITICAL
R-006	No centralized logging or SIEM	Monitoring	8.3	CRITICAL
R-007	Database backups not encrypted	Data Protection	8.2	CRITICAL
R-008	No incident response plan documented	Governance	8.0	CRITICAL
R-009	Backup verification not performed	Operations	7.8	HIGH
R-010	No network segmentation	Network	7.5	HIGH
R-011	Weak password policy (8 chars, no complexity)	Access Control	7.3	HIGH
R-012	Third-party vendor access unmonitored	Third Party	7.1	HIGH
R-013	No security awareness training program	People	5.3	MEDIUM
R-014	Endpoints missing EDR solution	Endpoint	6.8	HIGH
R-015	API keys hardcoded in source code	Development	7.9	HIGH

Note: This sample shows 15 of 47 identified risks. Full register includes detailed remediation guidance, affected assets, and compliance mapping for each risk.

RISK SCORING METHODOLOGY

Our risk scoring follows industry-standard CVSS methodology combined with business context specific to your organization. Each risk is evaluated on multiple factors:

Score Range	Priority	Required Action	Timeline
9.0 - 10.0	CRITICAL	Immediate remediation required	Within 7-14 days
7.0 - 8.9	HIGH	Prioritize for remediation	Within 30 days
4.0 - 6.9	MEDIUM	Plan for remediation	Within 90 days
0.1 - 3.9	LOW	Address as resources allow	Within 6 months

NEXT STEPS

1. Review the Risk Register with your security and IT leadership teams
2. Prioritize critical risks for immediate remediation
3. Reference the accompanying Remediation Roadmap for phased action plan
4. Schedule follow-up assessment in 90 days to validate progress