

CYBERSECURITY RISK ASSESSMENT

Risk register and remediation roadmap for a fictional SaaS business

Sample Portfolio Deliverable | Illustrative Price: \$999

FICTIONAL DEMONSTRATION — NOT AN ACTUAL CLIENT REPORT

Executive Summary

Sample client: BluePeak Analytics Inc., a fictional 55-person SaaS company handling customer business data in a cloud-hosted application.

The sample assessment identified eight material risks. Two are rated Critical/High and should receive immediate management attention: privileged-access exposure and incomplete incident-response readiness.

Assessment Approach

The demonstration organizes findings using NIST CSF 2.0 outcomes and a simple likelihood × impact model. Risk ratings are decision-support tools and should be adjusted to the client’s business context, contractual obligations and risk tolerance.

Risk Rating Scale

Score	Rating	Treatment Expectation
15-25	Critical/High	Immediate owner and treatment plan
8-14	Medium	Planned remediation with target date
1-7	Low	Accept, monitor or remediate as appropriate

Sample Risk Register

ID	Risk Scenario	L	I	Score	Rating	Treatment
RA-01	Compromise of privileged cloud account due to inconsistent strong MFA	4	5	20	High	Enforce strong MFA; separate admin accounts; quarterly access review
RA-02	Delayed containment	4	4	16	High	Approve IR plan; contact

	because response roles and escalation are undocumented					tree; tabletop exercise
RA-03	Unknown SaaS/data exposure due to incomplete asset inventory	3	4	12	Medium	Create authoritative asset/SaaS/data inventory
RA-04	Critical vulnerability remains open beyond business tolerance	3	4	12	Medium	Define severity SLAs and exception process
RA-05	Third-party compromise impacts customer data	3	4	12	Medium	Risk-tier vendors; collect evidence; track exceptions
RA-06	Recovery fails to meet business need	2	5	10	Medium	Define RTO/RPO and test restores
RA-07	Security logging misses relevant cloud events	2	4	8	Medium	Document log sources, retention and alert ownership
RA-08	Staff falls for targeted phishing	2	3	6	Low	Awareness program plus technical email protections

Top Recommendations

- Identity: enforce strong MFA and separate privileged administration from daily-user accounts.
- Governance: establish risk ownership, review cadence and documented acceptance/exception process.
- Incident response: document roles, escalation, evidence preservation and communications.
- Vulnerability management: define severity-based remediation targets and exception approval.
- Third-party risk: classify vendors by data/access/criticality and review security evidence accordingly.

90-Day Roadmap

Period	Management Objective	Example Outputs
0-30 days	Reduce immediate identity and response exposure	MFA enforcement, admin inventory, IR plan
31-60 days	Improve visibility and repeatability	Asset inventory, vulnerability SLAs, vendor tiers
61-90 days	Test and govern	Restore test, tabletop exercise, risk review meeting

Deliverables

- Executive summary
- Scoped control/evidence review
- Risk register with likelihood and impact
- Prioritized recommendations
- 90-day remediation roadmap
- Findings review meeting

Limitations

This sample is illustrative. A real assessment requires agreed scope, evidence, interviews and client-specific risk criteria. It does not certify compliance or replace a formal audit, penetration test or legal review.