



SAMPLE CONTROL PAGE

Vulnerability Management

A sample operating record for prioritizing security weaknesses, directing remediation, and documenting risk decisions.

Vulnerability Management

A practical, risk-based view of known security weaknesses, ownership, remediation progress, and decisions that require leadership attention. This sample is designed to show the type of operating record Unboredly can help organizations maintain.

Control objective	Identify, prioritize, remediate, and document vulnerabilities in a manner proportionate to business impact, exploitability, asset exposure, and available resources.
--------------------------	--

Executive snapshot

Open critical 2 Target: remediate within 7 days	Open high 8 Target: remediate within 30 days	Past due 3 Owner action required	Remediation rate 84% Rolling 90-day completion
--	---	---	---

Current risk register

Risk / finding	Asset / scope	Severity	Owner	Target	Disposition
Unsupported browser extension with excessive permissions	Sales workspace	Critical	IT Operations	Oct 09	Remove and verify managed-browser policy
Publicly exposed test storage container	Cloud test environment	Critical	Engineering	Oct 11	Restrict access; validate no sensitive data was stored
Endpoint patch level below approved baseline	12 managed endpoints	High	IT Operations	Oct 28	Patch window scheduled; exception review for 2 devices
Inactive third-party account remains enabled	Finance SaaS	High	Finance Systems	Oct 18	Disable account and confirm offboarding control

Decision and remediation cadence

Weekly: Review critical and high findings, confirm owners, update due dates, and remove blockers. Monthly: Review trend, aging, exceptions, and material residual risk with leadership. Quarterly: Validate the risk rating method, test evidence quality, and confirm that remediation priorities still align with the business.

Leadership decision required	Approve a time-bound exception for two legacy endpoints that cannot be patched until the planned application upgrade. Compensating controls: restricted access, enhanced monitoring by the IT provider, and a documented retirement date.
-------------------------------------	---

Minimum evidence retained

Evidence item	Example record
Finding source	Internal review, provider report, or approved security assessment
Risk decision	Severity, business impact, owner, treatment decision, and approval
Remediation evidence	Patch confirmation, configuration record, ticket closure, or validation note
Exception evidence	Business justification, compensating controls, approver, expiry, and review date