Risk acceptance form

Remediation vs Mitigation, edition 19 Nov 2026, https://remediationvsmitigation.com/risk-acceptance-form/.
License CC BY 4.0.

Risk Acceptance Form

Form version 1.0, first published 19 Nov 2026. License: CC BY 4.0. Cite as: Remediation vs Mitigation, Risk Acceptance Form, 19 Nov 2026, remediationvsmitigation.com/risk-acceptance-form/. Write no exploit steps, payloads or probing instructions in this record.

A. The finding

Field 1. Exception ID (your own number): _____ CVE ID(s) and scanner finding ID(s) covered: _____

Field 2. First detected (date, time, tool or report): _____ Evaluation completed (date, time): _____

B. Where it sits and how likely it is to be used

Field 3. Asset(s) or system ID(s): _____ Environment: [ ] prod [ ] dev Exposure: [ ] public [ ] internal Asset type: [ ] server [ ] application [ ] network device Field 4. Internet-reachable? [ ] yes [ ] no Basis (test or architecture drawing): _____ Field 5. Likely exploitable? [ ] yes [ ] no Reason: _____ On the CISA KEV catalog? [ ] yes [ ] no Catalog version checked: _____ Field 6. Estimated impact if exploited, on your own scale: _____

C. The decision

Field 7. Why this is accepted instead of fixed or mitigated: _____ Field 8. Mitigating factors and compensating controls in place (control, owner, how verified, date verified, entry link): _____ Field 9. Plan: corrective tasks, owner of each task, resources, milestones, scheduled completion dates: _____ Field 10. Reopen this record when: _____ Review every _____ days. Next review: _____ Field 11. Residual risk after the controls (one sentence) and the risk tolerance it is compared with: _____ Field 12. Only if the fix depends on a vendor: product, vendor status evidence, last vendor check-in date, next check-in date: _____

D. Decision and expiry

Field 13. Approver name, title, signature, date: _____ Statement: "I accept the residual risk in Field 11 until the date in Field 14." Field 14. Expiry date. The exception lapses on this date unless the approver renews it in writing: _____

E. Only if PCI DSS applies

Field 15. Compensating control worksheet: attach the worksheet your QSA uses, and name the PCI DSS requirement it stands in for: _____