EXECUTIVE SUMMARY TEMPLATE

From Technical Report to Business Decision

A side-by-side comparison and fill-in template

THE PROBLEM: TRADITIONAL vs. BUSINESS-ALIGNED

Most executive summaries lead with methodology and technical metrics. A business-aligned summary leads with impact and decisions.

✘ Traditional Executive Summary	✔ Business-Aligned Executive Summary
Methodology & Scope ACME Corp engaged [Firm] to perform an external network penetration test of 12 IP addresses and 3 web applications from March 3–14, 2026. Testing was conducted using the OWASP Testing Guide v4 and PTES methodologies. The assessment was performed from a black-box perspective with no prior credentials.	**Risk Exposure Summary** During this engagement, we identified findings representing an estimated $5.2M–$11.4M in aggregate risk exposure across three categories: regulatory penalties, operational disruption, and contractual liability. Two findings exceed ACME Corp's stated risk appetite of $1M annual cyber loss.
Results Overview The assessment identified 47 total findings: 3 Critical, 8 High, 19 Medium, 12 Low, and 5 Informational. The overall risk rating is High. The following chart shows the distribution of findings by severity: *[CVSS distribution chart]*	**Priority Decisions Required** 1. Customer database exposure (SQL injection): $3M–$8M regulatory risk. Requires 1–2 sprint development cycle. Compensating control deployable within 48 hours. 2. Partner data vulnerability (IDOR): $1.5M–$4M contractual exposure affecting 53 partners. Fix estimated at 2–4 hours of development. 3. Authentication weakness: Lateral path to ERP system ($40M annual revenue). Phase 1 mitigation achievable in <1 day.
Recommendations We recommend remediating all Critical and High findings as soon as possible. Medium findings should be addressed within 90 days. Low and Informational findings should be addressed as resources permit.	**Remediation Roadmap** We recommend a three-phase approach sequenced by risk reduction per effort. Phase 1 (week 1) addresses the two items exceeding risk appetite and reduces total exposure by approximately 70%. Full roadmap with effort estimates, dependencies, and projected risk reduction at each stage is provided in Section 4.

WHY THIS WORKS

The traditional summary answers: "What did we test and what did we find?"

The business-aligned summary answers: "What could hurt us, how badly, and what should we do first?"

One gets filed. The other gets forwarded to the board.

FILL-IN TEMPLATE: BUSINESS-ALIGNED EXECUTIVE SUMMARY

Copy this structure into your next report. Replace bracketed items with engagement-specific details.

RISK EXPOSURE SUMMARY

During this engagement, we identified findings representing an estimated [$ range] in aggregate risk exposure across [list categories: regulatory penalties, operational disruption, contractual liability, customer churn, etc.]. [Number] findings exceed [Client Name]'s stated risk appetite of [$ threshold].

Tip: If the client hasn't defined a risk appetite, use an industry benchmark and note it: "Based on industry benchmarks for organizations of similar size and sector, estimated acceptable annual cyber loss is approximately [$ figure]."

PRIORITY DECISIONS REQUIRED

List the top 3–5 findings in priority order. For each, include:

- What's at risk (asset + data + business function)
- Potential financial / regulatory / operational consequence (with $ range)
- Estimated remediation effort
- Compensating controls available (if any) and their risk reduction

Example:

1. [Title framed as business impact]: [$X–$Y] [risk type] exposure. Affects [system] which [business function]. Remediation requires [effort estimate]. Compensating control [available/not available] — deployable in [timeframe] for approximately [X%] risk reduction.

REMEDIATION ROADMAP

We recommend a [number]-phase approach sequenced by risk reduction per effort:

Phase 1 ([timeframe]): Address findings exceeding risk appetite. Estimated risk reduction: [X%]. Includes: [Finding titles].

Phase 2 ([timeframe]): Address high-impact items with moderate effort. Estimated cumulative risk reduction: [X%]. Includes: [Finding titles].

Phase 3 ([timeframe]): Address remaining findings and implement long-term controls. Estimated cumulative risk reduction: [X%]. Includes: [Finding titles].

Tip for external providers: Frame this as "recommended sequencing" rather than a prescriptive plan. Add: "We recommend reviewing this roadmap with your internal teams to adjust for sprint capacity and change management requirements."

RISK TREND (For Recurring Engagements)

Compared to [previous engagement date], total risk exposure has [increased/decreased] by approximately [X%]. Key changes: [list improvements and new risks]. Mean time to remediate for business-critical findings [improved/worsened] from [X days] to [Y days].

Tip: This section is only applicable for recurring engagements, but it's incredibly powerful. Even after a second engagement, trend data transforms the conversation from "here's what we found" to "here's how the program is performing."

FINDING SUMMARY TABLE

Replace the traditional severity-sorted list with a business-impact-sorted table:

Finding	Business Impact	Est. Financial Exposure	Remediation Effort	CVSS	Recommended Phase
[Title]	Critical	[$X–$Y]	[Effort]	[Score]	Phase 1
[Title]	High	[$X–$Y]	[Effort]	[Score]	Phase 1
[Title]	Moderate	[$X–$Y]	[Effort]	[Score]	Phase 2

Note: Business Impact tier (Critical/High/Moderate/Low) is determined by the contextual scoring methodology, not by CVSS alone. CVSS is included as a reference point but does not drive the prioritization.

This template is a companion resource to "How to Talk Cyber Risk with Nontechnical Stakeholders."