A ONE-PAGE TOOL

The Risk Translation Sheet

Turning a vulnerability report into something a business leader can act on — and act on differently depending on the answer.

Bhavin G Patel · C|CISO · CISSP-ISSAP · CISM

A vulnerability count is an activity measure. It tells the business how hard you are looking, not how exposed they are. Translation is the work of converting a technical finding into a sentence about the business that changes a decision. Use this sheet per finding, or per group of findings that share a consequence.

1 · The translation

Technical finding	
What an attacker gets	
Which business process stops, degrades or leaks	
Who feels it — customers, regulator, staff, market	
The business sentence	

> **THE TEST**
> The business sentence must contain no security vocabulary and must be falsifiable. “An attacker with a phished mailbox could approve their own supplier payment” passes. “Elevated risk of financial fraud” does not.

2 · Scoring that survives challenge

Dimension	Question	Score
Reachability	Can it be reached from the internet, or does it need a foothold first?	
Exploitability	Is it being exploited in the wild today, or is it theoretical?	
Blast radius	One system, one business unit, or everything?	
Compensating controls	What already reduces this, and is it verified or assumed?	
Data exposed	Classification, volume, regulatory status.	

A high-severity finding on an isolated system with a verified compensating control ranks below a medium finding on an internet-facing service holding customer data. Severity scores from a scanner do not know that. You do.

3 · What you are actually asking for

Ask	Use when
Fix it	Cost is proportionate and an owner exists. Give a date, not a priority.
Fund it	The fix needs resource the owner does not have. Name the amount and what it buys.
Accept it	The fix costs more than the exposure. Needs a named accepting owner and an expiry date.
Decide it	Two legitimate options with different business consequences. Present both, recommend one.

4 · Reporting that changes behaviour

Report this	Not this
Exposure by business service, with the worst case stated	Total open vulnerabilities
Time to remediate, split by whether it was automated	Percentage patched
Findings past their agreed date, by owner	Findings by severity
Risks accepted, by whom, expiring when	Risk register size
What we stopped doing to do this	Activity completed

> **THE NUMBER THAT UNDERMINES YOU**
>
> Reporting a rising vulnerability count as evidence of a problem, then a falling one as evidence of success, teaches the board that the metric measures your effort rather than their exposure. Pick the exposure framing once and hold it, even in the quarter when it looks worse.

Companion to: “Stop Reporting Vulnerabilities. Start Reporting Risk.” at cybersecleader.com. Adapt freely inside your organisation with attribution retained. Not legal or regulatory advice.