# THE CONSEQUENCE MULTIPLIER™

*Four Questions That Transform Any Audit Finding Into Executive Action*

*Most audit findings are ignored not because the problem is unimportant — but because the Consequence was written too vaguely for executives to feel the urgency.*

**Run every Consequence statement through these four questions before you submit.**

| # | THE QUESTION | WHAT TO LOOK FOR | EXAMPLE (IAM Finding) |
|---|---|---|---|
| 1 | **What specifically could go wrong?**<br><br>*Not 'unauthorized access' — which data, which systems, which users?* | Name the data type at risk: PII, financial records, health data, intellectual property.<br><br>Name the specific systems: Active Directory, ERP, payment processing, customer database.<br><br>Identify which users or roles are exposed. | *"The 520 excess accounts and 54 unauthorized accounts represent active attack vectors providing potential access to financial records, PII, and proprietary business data."* |
| 2 | **What does it cost?**<br><br>*Find a published figure. Cite your source.* | IBM Cost of a Data Breach Report (annual)<br>Verizon Data Breach Investigations Report (annual)<br>Regulator penalty schedules (PIPEDA, HIPAA, GDPR, PCI-DSS)<br>Industry-specific breach cost studies<br><br>**Use real numbers. Cite the source.** | *"The average cost of a data breach in Canada in 2024 was $6.32 million (IBM Cost of a Data Breach Report, 2024), not including reputational damage and customer attrition."* |
| 3 | **Is any part of this happening right now?**<br><br>*Not 'could happen' — is happening.* | Identify conditions that are active today, not theoretical future risks.<br><br>Look for: active accounts belonging to terminated employees, systems currently unpatched, data currently exposed, controls currently not operating.<br><br>**Present tense creates urgency. Future tense creates procrastination.** | *"23 accounts belonging to terminated employees are active right now, providing former employees with current access to organizational systems."* |
| 4 | **Which regulation or commitment is at risk?**<br><br>*Name it specifically.* | Canada: PIPEDA, provincial privacy laws<br>USA: HIPAA, GLBA, SOX, CCPA, state breach laws<br>International: GDPR, ISO 27001 certification<br>Industry: PCI-DSS, CMMC, client contract requirements<br><br>**State the specific penalty or consequence of non-compliance.** | *"The organization processes personal data subject to PIPEDA. A breach resulting from inadequate access controls may require notification to the OPC. Failure to notify carries penalties of up to $100,000 per violation."* |

**Remember:** The severity rating (High / Medium / Low) is a label. The Consequence is the argument. A High-rated finding with a one-line Consequence will be ignored. A Medium-rated finding with a specific, documented Consequence will get immediate action. Do not rely on the rating. Make the argument.



*© PI Sec Audit 2019–2026. For course use only. Not for redistribution.*