

You've just become responsible for security and there is no CISO

The five questions the board will ask: score yourself

Five questions, two points each. Score what is true today, not what is planned. Ten minutes, honestly, is worth more than an afternoon generously.

The board asks	0	1	2	Score
1 "If something goes wrong tonight, who decides what we do, and when do we hear about it?" <i>Who decides what, and what gets escalated to whom?</i>	Nobody can say who approves a risk exception	People know, but it is not written down or signed	Written, signed by the CEO, with thresholds and turnaround times	
2 "How much of this are we prepared to lose?" <i>What level of risk will we carry, in numbers an operating team can use?</i>	Adjectives only, or no statement	Numbers exist, but operations has never seen them	Three numbers an engineer can check against without calling anyone	
3 "Will this still work when the people who built it leave?" <i>How are standards written so they survive the next reorganisation?</i>	Cannot produce a list of standards with owners	A list exists, but more than one in ten owners has left, or nobody has a successor	Every standard has an owner, a successor and a review date	
4 "We passed the audit. How do you know it's actually working?" <i>Where does assurance come from between audits?</i>	The only control evidence anyone has seen was pulled by an auditor	Some evidence is collected, but the owners collect it on themselves	Scheduled, independent sampling; failures to the risk committee within thirty days	
5 "What should we be looking at, and how will we know if it gets worse?" <i>What does the board actually see, and how often?</i>	The board sees a different deck every time, or no regular update	Regular updates, but the metrics change	One page, the same three to five metrics every quarter, with the decisions asked for	
Total				/ 10

What the total means

0 to 3: a policy library. The policies exist; the decisions don't. Start with question 1: a one-page decision list, signed by the CEO. It costs a page and a signature.

4 to 6: a framework in parts. Usually questions 1 and 5 are done and 2 to 4 are missing. Start with question 3: the owner list tells you which standards are already orphaned.

7 to 10: governance. The remaining points are the ones a regulator, an insurer or a court would ask about first. Start with the lowest row.

The Monday list

- Write the decision list: five decisions, who makes each, the threshold, the turnaround in days. Get it signed.
- Put your last four board updates side by side. Circle the metrics that appear in all four.
- List every standard and its owner. Mark the ones whose owner has left.
- Take three questions to the CEO or the chair: how many hours down before the board hears; how much one incident can cost before the board hears; how many control failures a quarter before someone acts.
- Pick three controls you would be embarrassed to find broken. Pull the evidence yourself this month.

The five questions land differently in every organisation. Send me your score, and I'll tell you which of the five I would look at first in yours. Twenty minutes, no deck, nothing to prepare.

ilya@irongateitconsulting.com.au · [linkedin.com/in/ilya-polyakov](https://www.linkedin.com/in/ilya-polyakov)