SORAMI / SECURITY

# vCISO monthly report: outline of the format

This is the shape of the report, not a filled-in example. The content is written against your risk register.

## The six sections

| Section | The question it answers | What goes in it |
|---|---|---|
| Risk register movement | Did our exposure change this month? | Risks opened, closed and re-rated, with the reason for each move. |
| Open findings | What is outstanding and who has it? | Findings by severity with a named owner and a due date each. |
| Compliance status | Where are we against each framework in scope? | Per framework: controls met, controls in progress, and the next external date. |
| Incidents and near misses | What went wrong, including what nobody escalated? | Each event with how it was detected. How long it ran, and what changed after it. |
| Vendor and access changes | Who can reach what, and what is new? | New and removed vendors, privilege changes, and access review results. |
| Decisions needed | What do we need from leadership this month? | Each decision, the options, the recommendation and the cost of waiting. |

## Rules the report follows

- One page of summary, then the detail. The summary is for the board.
- Every finding carries an owner and a date, or it is not in the report.
- Movement is shown against last month, not against a target we set once.
- Written so a customer or an auditor could read it without a translator.
- No severity is changed without the reason recorded in the register.

## What the report is not

- Not a dashboard export with no narrative attached.
- Not a list of tickets closed by the engineering team.
- Not an assurance opinion. We are not your auditor.
- Not a substitute for an incident report during an incident.

## Who reads it

The summary page is written for a board or a leadership group. The detail sections are written for the engineers who own the findings. A customer security reviewer can be sent the whole thing without editing, which is the point of keeping it plain.

Sorami Consulting Pty Ltd, ACN 702 116 452, Australia. hello@sorami.com.au. Outline of the report format. Not a client report.