WHAT THE ROLE COVERS

Virtual CISO · role overview

One person holds the security role. Requests reach it from every side: an engineer during a design review, compliance with a customer questionnaire, support after an alert, management before a board meeting. This document sets out the work that passes through the role and the instrument used to measure it.



DIRECTION	EXAMPLES OF WORK DONE
Governance, risk and compliance decisions, risk and the paper trail	• Turned a regulation into a list of obligations with a named owner for each one • Brought a risk the board had accepted back to them when the condition it was accepted under expired
Security operations changes to the environment	• Set the security requirements for a data migration, then verified afterwards that the environment could not be reached from outside • Defined who answers an alert out of hours, and what they may do
Security architecture, design and development new products and systems	• Set security requirements for a new service before the build started • Changed an integration design so that a failure in one component could not reach customer data

These are the usual names for three areas of security practice, not a numbered list from a framework. The role also covers training, privacy, continuity, procurement, budget and hiring.

ONE FINDING, THREE AREAS OF WORK

Findings rarely stay inside one area. A single one usually needs work in all three, and the role covers all three rather than passing part of it on or waiting for someone to be found for it.

> THE FINDING
> Developers held standing administrative access to production

AREA	WHAT HAPPENED
Security operations	Found while reviewing who can reach what; the exposure was confirmed by attempting access without a request
Security architecture, design and development	Access was redesigned to be granted per task and logged, and the change was built into the release process rather than handled as an exception
Governance, risk and compliance	Entered the register with a named owner and a review date, and was re-scored only after the new control had been tested

The same person carried this from the first observation to the closed line in the register. Who does the work depends on the task: the client's team, practitioners already contracted alongside the role, or someone recruited into the team when the need is continuous.

Where the boundary sits. The role sets the security requirement, defines the framework and roles, and verifies the result before accepting it. It does not administer systems day to day and does not replace the client's team.

HOW THE WORK IS MEASURED

Virtual CISO · role overview

The work described above is recorded in the risk register. A risk enters or moves in it in one of three ways: newly discovered, reassessed, or verified once the control intended to reduce it has been tested. Each risk is closed in one of four ways by its named owner.



OUTCOME	WHAT IT LOOKED LIKE IN PRACTICE
Mitigated	Backups could be deleted with ordinary administrator credentials; a separate copy was added that cannot be removed from the main environment, and the control was tested by attempting deletion
Minimised	Vulnerable components could not all be removed at once, so fix deadlines entered the release process and the most exposed services were done first
Accepted	Evidence was held in several places and consolidating it was not affordable that year; the owner signed for the risk with an expiry date and a quarterly check
Avoided	An integration that would have given a supplier direct access to customer data was dropped in favour of a data feed with no return path

HOW THE REGISTER IS KEPT

- Risks are re-scored when a control is tested, not when it is installed.
- An incident, a major change, a new supplier or a new regulation triggers a review outside the normal cycle.
- Every accepted risk carries an expiry date, so acceptance is revisited rather than becoming permanent.
- Indicators are selected for the specific environment rather than taken from a standard list.
- When an indicator moves in the wrong direction, it is raised at the next management review with its cause and a proposed response.
- The register is maintained continuously and stays with the client.

More about the role: defencelab.io/vciso · contact@defencelab.io