VYFORITY

Cyber security and business architecture advisory

Questionnaires measure confidence. *We measure posture.*

Most cyber assessments ask your team how things are configured, then grade the answers. Vyfority's readiness assessment inspects the environment itself: external scanning, configuration analysis and evidence review against the benchmark you choose, so your board sees what is true rather than what is reported.

Evidence, not assertion

Scanning and configuration analysis test what interviews and documents claim. The gap between the two is usually where the material risk lives.

Your benchmark, not ours

Essential Eight, NIST CSF, ISO 27001, CIS Controls, or the standard an insurer, customer or regulator holds you to. You choose what "ready" means.

Posture across four lenses

Governance, people, process and technology, assessed together, because real incidents pass through all four.

THE PROBLEM WITH SELF-REPORTED SECURITY

Green on the dashboard is not green underneath

Most executives have seen the pattern: status reports **green**, tools purchased, boxes ticked. Then an insurer, a major customer or an incident asks one precise question, and nobody can evidence the answer. It is the watermelon problem: **green** outside, **red** inside, and questionnaire-based assessments industrialise it. They grade what people believe, and belief is exactly what an attacker never tests.

WHAT AN ASSESSMENT SHOULD GIVE A BOARD

The material risks. Not four hundred findings: the handful that could genuinely hurt the organisation, expressed in business terms a board can weigh and a CFO can price.

The true posture. Where reported controls hold up under inspection and where they quietly don't, mapped across governance, people, process and technology.

A path you can actually walk. A sequenced, practical roadmap sized to your team and budget, not an enterprise wish list that dies in the next planning cycle.

The independence that makes it credible. Vyfority does not resell security products and does not operate your systems, so the findings carry no sales agenda. When the right answer is "keep what you have and configure it properly", that is the finding. An assessment from your MSP or a vendor is homework marked by the people who did it.

THE METHOD · FIXED FEE, AGREED SCOPE

01

Frame

Select the benchmark and agree scope and depth up front. The assessment answers the question **your** board, insurer or customer is actually asking, not a generic maturity survey.

02

Evidence

External attack-surface scanning, configuration analysis of the platforms that matter (identity, email, endpoints, cloud), and structured document and interview review. Every claim triangulated against what the environment actually shows.

03

Findings

Material risks ranked in business terms and posture mapped across the four lenses, delivered in a plain-language executive debrief. No jargon that needs an interpreter, no fear theatre.

04

Roadmap

Prioritised and sequenced: quick wins first, structural work staged, each step with an owner and realistic effort. Includes a **board-ready summary you can table as-is**.

Know where you stand before someone else tells you

The next people to test your posture will be an insurer, a major customer, an auditor or an attacker. A readiness assessment means the first honest inspection happens on your terms. Fixed fee, agreed before we start, led personally by a former enterprise CISO.

Dean Kastelic · Founder, former enterprise CISO
dean.kastelic@vyfority.com.au
linkedin.com/in/deankastelic · vyfority.com.au