VYFORITY

Cyber security and business architecture advisory

Regulation is stacking up. *Your framework shouldn't.*

The 72-hour ransomware reporting clock, SOCI obligations, Privacy Act reform, APRA's prudential standards and its supervisory expectations on AI, the new Aged Care Act. Treated as separate projects, each produces a binder. Vyfority builds one governance framework mapped to controls and verified across the three lines of assurance: a single body of evidence that answers every regulator, including in the 72 hours that matter most.

72 hours

Ransomware payment reporting under the Cyber Security Act 2024 for organisations at $3M+ turnover. A civil penalty regime, and a clock that tests preparation, not paperwork.

One framework, many regimes

Obligations from the Cyber Security Act, SOCI, the Privacy Act, APRA CPS 234 and CPS 230, and aged-care reform, traced to a single control set. Build once, evidence many.

Three lines, actually tested

Controls verified across the three-lines assurance model: management checks, risk oversight, independent testing. "Compliant" becomes a statement of evidence, not intent.

THE MID-MARKET REGULATORY SQUEEZE

The binder problem

Each new regime arrives as its own project, its own consultant, its own binder. The result: overlapping policies nobody reads, controls asserted but never tested, and a board assured "we're compliant" with nothing behind the word. It is the watermelon problem in a folder: **compliant** on the cover, **untested** inside. And when an incident starts the 72-hour clock, binders do not answer regulators. Evidence and rehearsed decisions do.

WHAT THE FRAMEWORK GIVES A BOARD

One regulator-mapped framework. Every obligation that applies to you, from the Cyber Security Act to APRA's AI expectations to the new Aged Care Act, traced to a single set of controls aligned with your risk framework. The next regulation becomes a mapping exercise, not a project.

Compliance you can evidence. A testing and verification schedule across the three lines of assurance, with an evidence repository behind every asserted control. When a regulator, auditor or insurer asks "show me", there is something to show.

A response you have rehearsed. The 72-hour obligations wired into an incident playbook: decision rights settled, notifications drafted, reporting paths tested before they are needed at 2am.

The fractional route to done. Compliance programs stall for lack of a senior owner, not intent. An optional fractional retainer puts a former enterprise CISO in your leadership cadence at a fraction of a hire: driving the framework to done and briefing the board.

THE METHOD · FIXED FEE TO BUILD, OPTIONAL RETAINER TO RUN

01

Map

Establish which regimes capture you and build the obligations register: Cyber Security Act, SOCI, Privacy Act, APRA standards and AI expectations, aged-care reform. Gap-assess today's state.

02

Build

One governance framework aligned to your internal risk framework: policies people can follow, each control mapped to the obligations it satisfies, ownership assigned where the work happens.

03

Verify

Testing across the three lines: management self-checks, risk oversight, independent verification, scheduled by control criticality. Evidence repository maintained; **board reporting directors can read**.

04

Respond

The 72-hour playbook built and exercised: roles, decisions, draft notifications, regulator paths. An optional **fractional senior-leader retainer** keeps the capability warm.

Be ready before the clock starts

Every regime above is already law or already landing; the only variable is whether you meet it with one framework or five binders. Fixed fee to build, optional fractional retainer to run, led personally by a former enterprise CISO and ex-KPMG Director of Cyber Advisory who has sat on the regulated side of the table.

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