VYFORITY

Cyber security and business architecture advisory

You can outsource the service. *You can never outsource the risk.*

Your business now runs on other people's systems: cloud, SaaS, outsourced operations, and the suppliers behind those suppliers. Vyfority runs third and fourth party risk as a managed service: a defensible register, proportionate assessments verified with OSINT scanning, and scheduled reassessment, so supplier risk is governed continuously rather than surveyed once and filed.

Verified, not just surveyed

Every questionnaire response is checked against OSINT scanning of the supplier's external posture. Suppliers self-report generously; the internet does not.

Proportionate by design

Assessment depth scaled to each supplier's risk, size and service type: cloud, outsourcing, SaaS or other. No 300-question form for the stationery supplier.

Managed, not a project

The function runs on a schedule with fast turnarounds and ongoing reassessment: vendor-risk capability without the headcount to justify.

WHY SUPPLIER RISK IS NOW BOARD RISK

"Show me the supplier register" has no good improvised answer

The pattern behind Australia's most damaging breaches is entry through a supplier, and the accountability has followed the pattern. CPS 234 makes information held by third parties the regulated entity's problem, and its flow-down means mid-market firms now receive the questionnaires whether regulated or not. Enterprise customers, funding bodies and insurers embed the same demands in contracts. When any of them, or an incident, asks who holds your data and how you know they protect it, the answer is either a register or an apology.

WHAT THE MANAGED SERVICE GIVES A BOARD

A defensible register. Material suppliers identified and tiered in alignment with CPS 234 and your internal risk framework, including the critical fourth parties behind them, where concentration risk hides.

Assessments that hold up. Vyfority's proprietary questionnaire or your own, sized to the supplier, verified with OSINT, and turned around fast enough that procurement never stalls waiting on security.

A living picture. Scheduled reassessment and onboarding checks for new suppliers, so the board's view of supplier risk is current, not a PDF from two renewal cycles ago.

No platform agenda. Vyfority does not resell a TPRM platform priced per vendor, so there is no incentive to inflate your supplier count, your assessment depth or your subscription tier. The register holds what is material, assessments go as deep as the risk warrants, and the fee reflects the work.

THE SERVICE · MONTHLY, SCOPED TO YOUR SUPPLIER BASE

01

Register

Identify and tier your material suppliers in alignment with CPS 234 and your internal risk framework, and map the critical **fourth parties** behind them. The register becomes the governance backbone everything else hangs off.

02

Assess

Proportionate questionnaires (Vyfority's proprietary set or your custom one) tailored to each supplier's scale, risk level and service type: cloud, outsourcing, SaaS or other. Responses verified against OSINT scanning, with fast turnaround.

03

Deepen OPTIONAL

For critical suppliers: review of cyber contract clauses against what the assessment actually found, and solution architecture assessment where a supplier is embedded deep in your operations.

04

Maintain

Scheduled reassessment on a cycle matched to each tier, onboarding assessment for every new material supplier, and **board-legible reporting** on the state of the supplier estate.

The supplier questions are coming either way

From a customer's procurement team, an insurer's renewal form, a regulator, or an incident in someone else's network. A managed service means the register exists, the assessments are current and the answers are ready before anyone asks. Monthly fee, scoped to your supplier base, overseen personally by a former enterprise CISO.

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