VYFORITY

Cyber security and business architecture advisory

The Cyber Deal Breaker *Checklist*

Ten checks to run against a target's data room. A management team is incentivised to present cyber risk favourably during a transaction, and standard IT diligence checks licences and server counts rather than liability. Each unanswerable item is either a negotiating lever or a post-close cost you will carry.

Ten checks
Run during data room review, before the technical diligence scope is set.

Three or more unanswered?
The target is carrying technical debt that has not been priced into the deal.

CHECKS 01-04 What the data room will not show you

Outside-in signals the target cannot curate, and rarely volunteers.

- ☐ **01 Credential exposure**
  Have you checked whether the target's senior staff credentials appear in known breach dumps? **An outside-in check needs no cooperation and is rarely already known internally.**
- ☐ **02 Internet-facing exposure**
  Can you see what the target exposes publicly: remote access, forgotten subdomains, unpatched edge devices? **The external footprint is the attacker's starting point and yours.**
- ☐ **03 Undisclosed incident history**
  Is there public evidence of a prior incident that does not appear in the data room? **Non-disclosure is itself a finding, and a warranty question.**
- ☐ **04 Shadow estate**
  Do the asset and licence registers reconcile with what is actually running, including anything acquired in the target's own prior deals? **Unmapped systems are unpriced systems.**

CHECKS 05-07 The assurance that is not assurance

Certificates and test reports are routinely scoped to say very little.

- ☐ **05 Certification scope**
  Does the ISO 27001 or equivalent certificate cover the systems that actually run the business? **Scope statements routinely exclude the operating estate.**
- ☐ **06 Penetration test reality**
  Have you read the test scope and the retest, not just the summary? **"No critical findings" often means a narrow scope, an old date, or unremediated criticals downgraded.**
- ☐ **07 Recovery, evidenced**
  Has the target restored a material system end to end and recorded the time? **Backup success rates say nothing about recovery capability, which is what a claim turns on.**

CHECKS 08-10 The liabilities that transfer with the entity

Obligations and exposures that become yours at completion.

- ☐ **08 Regulatory obligations**
  Does the target carry obligations that transfer at completion: SOCI, Privacy, sector regimes, or the 72-hour ransomware reporting duty? **You inherit the duty and the record of how it was met.**
- ☐ **09 Supplier concentration**
  Which third and fourth parties hold the target's data, and can any of them be terminated or repriced on change of control? **Contract terms surface here or they surface after close.**
- ☐ **10 The costed remediation number**
  The one that changes the price. Can you state, in dollars, what it will cost to bring the target to an acceptable posture in year one? Without that figure you are negotiating on adjectives.

HOW DID YOU SCORE?

9–10	Diligence is doing its job. Price the residual and proceed.
6–8	Material unknowns. Scope technical diligence before the term sheet hardens.
Under 6	You are pricing an asset you cannot see. Quantify before you commit.

Cyber diligence, at deal speed

An **OSINT Red Flag Scan** answers checks 01 to 04 from the outside in, before you commit to deeper diligence. Where the picture warrants it, a full **Cyber Diligence Sprint** produces a Costed Remediation Roadmap: the dollar figure you take to the negotiation.

All briefings under NDA. Fifteen minutes to discuss an active target or a portfolio requirement.

BOOK A DEAL BRIEFING →

Dean Kastelic · former enterprise CISO · ex-KPMG Director
dean.kastelic@vyfority.com.au · vyfority.com.au