How Secure Is Your IT Strategy?
A 10-Point Self-Assessment for Mid-Market Leaders

Think your IT strategy is covered?

Most mid-market companies discover dangerous gaps only after a costly breach or outage. This **10-point self-assessment** reveals if your IT and security strategy is truly resilient—or if blind spots are putting your business at risk.

10 Questions That Reveal Your Hidden IT Risks

1. Do your IT and security providers share a unified incident response plan? — ☐ Yes ☐ No

2. Are your systems monitored 24/7 by the same team that maintains them? — ☐ Yes ☐ No

3. Do you have one accountable partner for both IT performance and security risk? — ☐ Yes ☐ No

4. Can your IT/security teams resolve incidents without vendor finger-pointing? — ☐ Yes ☐ No

5. Is security built into your IT environment by design—not bolted on later? — ☐ Yes ☐ No

6. Do you have full visibility into all assets, users, and vulnerabilities? — ☐ Yes ☐ No

7. Are your compliance requirements actively mapped into your IT operations? — ☐ Yes ☐ No

8. Do you know your true cost of downtime per hour? — ☐ Yes ☐ No

9. Are all your security tools integrated—or are they scattered across multiple vendors? — ☐ Yes ☐ No

10. Do you test your disaster recovery & business continuity plans regularly? — ☐ Yes ☐ No

Scoring Section

(0–3 YES)　(4-7 YES)　(8–10 YES)

0–3 YES:
High risk. Immediate action is needed to protect your business.

4–7 YES:
Gaps are lurking. A breach or outage could expose you at any time.

8–10 YES:
You're ahead of the curve. But even well-managed IT benefits from a proactive security review.

If you scored below 8, your IT strategy has hidden risks.

Let's identify and eliminate them before an attacker does.

Schedule your free Security Consultation