IT Risk Strategic Assessment

Executive Oversight • Cybersecurity • Business Continuity • Cost Control

Section 1: Governance & Strategic Alignment

☐ **Strategic Roadmap:** Is there a 12–24 month technology plan that supports business growth rather than just reacting to failures?

☐ Independent Audit: Has an entity other than your primary IT provider reviewed your security posture in the last 12 months?

☐ Budget Clarity: Is there a documented capital expenditure (CapEx) plan for hardware and software lifecycles?

Cybersecurity Foundations

☐ MFA Everywhere: Is Multi-Factor Authentication mandatory for email, VPNs, and all financial/SaaS portals?

☐ Backup Immutability: Are backups stored in a way that they cannot be deleted or encrypted by a ransomware actor?

☐ Offboarding Protocol: Is there a formal process to revoke all digital access within one hour of an employee termination?

Business Continuity

☐ Defined RTO/RPO: Has leadership documented exactly how much data loss or downtime (in hours) the firm can financially sustain?

☐ Redundancy: If your primary office internet or server fails, is there an automated failover in place?

☐ Insurance Alignment: Have you reviewed your Cyber Insurance policy to ensure your current tech stack meets their minimum requirements for a payout?

Vendor & Cost Control

☐ MSP Accountability: Does your IT provider provide monthly reports on uptime, ticket trends, and patch compliance?

☐ License Optimization: Are you paying for ghost licenses for software or users that are no longer active?

☐ Contractual Flexibility: Are you aware of your contract's Notice of Non-Renewal period to avoid automatic multi-year lock-ins?