Cyber Defense. Audit-Ready.

Cybersecurity & Compliance Readiness Questionnaire

For Owners, CEOs, CIOs, CISOs, and Executive Leadership Staff

Prepared by R32 Solutions (R32) 2025

Mission Critical Cybersecurity & Compliance Readiness Questionnaire

1. Governance & Oversight

1. ☐ Yes ☐ No — Does the organization have a documented cybersecurity and data governance program aligned with NIST and/or ISO/IEC 27001?
2. ☐ Yes ☐ No — Is a CISO or equivalent responsible for cybersecurity oversight?
3. ☐ Yes ☐ No — Are cybersecurity policies formally approved by executive leadership or the board?
4. ☐ Yes ☐ No — Has the organization conducted a formal risk assessment in the last 12 months?

---

2. Access Control & Identity Management

5. ☐ Yes ☐ No — Are user access controls based on the principle of least privilege?
6. ☐ Yes ☐ No — Does the organization use multi-factor authentication (MFA) for privileged access?
7. ☐ Yes ☐ No — Are user accounts reviewed and deprovisioned promptly upon termination?

---

3. System Security & Infrastructure

8. ☐ Yes ☐ No — Are all systems and software regularly updated and patched?
9. ☐ Yes ☐ No — Is there centralized logging and monitoring of security events (e.g., SIEM)?
10. ☐ Yes ☐ No — Are backups encrypted, tested, and stored securely offsite or in the cloud?

---

4. Incident Response & Threat Management

11. ☐ Yes ☐ No — Is there an incident response plan that includes ransomware and data breach scenarios?
12. ☐ Yes ☐ No — Has the organization conducted a tabletop or live incident response exercise in the past year?
13. ☐ Yes ☐ No — Are cybersecurity threats and vulnerabilities tracked and remediated through a defined process?

---

5. Compliance & Audit Readiness

14. ☐ Yes ☐ No — Does the organization maintain compliance with one or more frameworks (e.g., HIPAA, CMMC, NIST, ISO)?
15. ☐ Yes ☐ No — Are internal or external audits conducted at least annually to assess cyber and compliance readiness?
16. ☐ Yes ☐ No — Are records and documentation available for regulatory or certification review upon request?

---

6. Workforce & Awareness

17. ☐ Yes ☐ No — Are employees trained annually on cybersecurity awareness and compliance responsibilities?
18. ☐ Yes ☐ No — Are simulated phishing or social engineering campaigns conducted to evaluate user resilience?

---

7. Third-Party & Supply Chain Security

19. ☐ Yes ☐ No — Are third-party vendors evaluated for cybersecurity risk prior to engagement?
20. ☐ Yes ☐ No — Are business associate agreements (BAAs) or equivalent cybersecurity terms in place with critical vendors?