Free Cyber Readiness Checklist

Use this checklist to quickly assess your organization's foundational cybersecurity posture. This is a

high-level readiness guide—not a compliance audit.

People & Awareness

- Employees receive regular cybersecurity awareness training
- Phishing and social engineering risks are addressed in training
- Staff know how to report suspicious activity
- New hires receive security onboarding

Technology & Infrastructure

- Systems and software are regularly patched
- Antivirus/EDR is installed and monitored
- Regular data backups are performed
- Backups are tested for successful recovery
- Devices use encryption

Policies & Governance

- Security policies are documented
- Policies are reviewed periodically
- Access is granted based on least privilege
- HIPAA / regulatory obligations are understood (if applicable)

Incident Response

- An incident response plan exists
- Roles and responsibilities are defined
- Incidents can be escalated quickly
- Past incidents are reviewed for lessons learned

Risk & Oversight

- Risks are identified and tracked
- Third-party vendors are reviewed for security risk
- Leadership is informed of cyber risks
- Cybersecurity is part of business decision-making

Next Step: Get a personalized maturity score and improvement roadmap by completing the RCA-50™

Cyber Readiness Assessment.