



Cybersecurity Readiness Checklist

A practical self-assessment to help identify common cybersecurity gaps and next-step priorities.

Organization	Primary Contact	Date	Completed By

How to use this checklist

Answer each question as honestly as possible. Mark one response for each item and add notes where clarification would be helpful. A “No” or “Unsure” response does not mean your organization has failed; it simply highlights an area that may warrant review, remediation, or planning.

Important note: Organizations that handle regulated or sensitive data—such as PII, financial data, healthcare data, tax information, or other protected records, may have security, privacy, retention, recovery, and reporting obligations beyond the scope of this checklist.

1. Endpoint and Email Security

Assessment Item	Yes	No	N/A	Unsure	Notes
Business-grade endpoint protection is installed and actively managed on all company-managed devices.	☐	☐	☐	☐	
Email security protections such as anti-phishing, anti-spam, and malware filtering are active for all business email accounts.	☐	☐	☐	☐	
Endpoint detection and response (EDR/XDR) or an equivalent managed security capability is in place to detect and remediate threats.	☐	☐	☐	☐	
Company devices are encrypted where appropriate, especially laptops and other portable devices.	☐	☐	☐	☐	
Employees are prevented from installing unauthorized or unnecessary software without approval.	☐	☐	☐	☐	

2. Identity and Access Management

Assessment Item	Yes	No	N/A	Unsure	Notes
Each user has a unique account for business systems; shared logins are avoided except where formally documented and controlled.	☐	☐	☐	☐	
A strong password policy is enforced, with long passwords or passphrases encouraged and support for password manager use.	☐	☐	☐	☐	
Multi-factor authentication (MFA) is required for email, VPN, remote access, administrator accounts, and other critical systems.	☐	☐	☐	☐	
Default passwords on firewalls, routers, printers, cameras, access points, and other connected devices have been changed.	☐	☐	☐	☐	
Access to systems and data is granted according to job role and limited to the minimum necessary level.	☐	☐	☐	☐	

3. Backup and Recovery

Assessment Item	Yes	No	N/A	Unsure	Notes
Critical business data is backed up on a defined schedule and protected from a single point of failure.	☐	☐	☐	☐	
At least one backup copy is isolated, immutable, offline, or otherwise protected against ransomware and unauthorized change.	☐	☐	☐	☐	
Backups are encrypted where appropriate.	☐	☐	☐	☐	
Backups are tested periodically by performing file-level and/or full restore checks.	☐	☐	☐	☐	

4. Network and System Management

Assessment Item	Yes	No	N/A	Unsure	Notes
All internet-connected locations are protected by a properly configured business-grade firewall.	☐	☐	☐	☐	
Operating systems, applications, firmware, and network devices are actively supported and kept current with security updates.	☐	☐	☐	☐	
There is an up-to-date inventory of devices, systems, and locations that store, process, or transmit sensitive business or client data.	☐	☐	☐	☐	
Guest Wi-Fi, if provided, has a non-obvious name, is segmented from the primary business network, and cannot access internal systems or data.	☐	☐	☐	☐	
Remote access tools and VPN connections are encrypted, approved, and protected with MFA.	☐	☐	☐	☐	

5. Policies, Governance, and Data Handling

Assessment Item	Yes	No	N/A	Unsure	Notes
The organization has a written information security policy or plan that is reviewed periodically and communicated to relevant staff.	☐	☐	☐	☐	
There is a designated person or role responsible for cybersecurity coordination and follow-up.	☐	☐	☐	☐	
Physical and digital access to sensitive data is governed by policy and enforced in practice.	☐	☐	☐	☐	
Former employees, vendors, or contractors have their access removed promptly when it is no longer needed.	☐	☐	☐	☐	

6. Awareness and Incident Preparedness

Assessment Item	Yes	No	N/A	Unsure	Notes
Employees receive cybersecurity awareness training, including phishing and social engineering guidance.	☐	☐	☐	☐	
There is a documented process for reporting suspicious emails, security incidents, lost devices, or suspected breaches.	☐	☐	☐	☐	
A breach or incident response plan identifies internal decision-makers and external points of contact as needed.	☐	☐	☐	☐	
Leadership knows who to contact for IT and cybersecurity assistance if an urgent issue occurs.	☐	☐	☐	☐	

Interpreting results

Items marked “No” or “Unsure” typically represent the highest-value starting points for follow-up. This checklist is intended to support discussion and prioritization; it is not a substitute for a formal security assessment, compliance review, or legal guidance.

Organizations handling Personally Identifiable Information (PII), Personally Identifiable Financial Information (PIFA), or Personally Identifiable Healthcare Information (PIHI), or those subject to IRS, HIPAA, or other regulations, may have additional security requirements not addressed by this checklist.

Need help reviewing your results?

GracemSP offers no-obligation consultation and practical guidance for security, backup, systems, and IT risk planning.
 215-536-0100