CTRL THE FUTURE LLC

CYBERSECURITY READINESS CHECKLIST

A practical self-review for organizational cybersecurity readiness

Purpose: Use this checklist to identify foundational cybersecurity strengths and areas that may require additional attention. It is designed as an initial readiness resource - not a substitute for a formal risk assessment, penetration test, compliance audit, or professional security review.

Organization: _____

Completed by: _____

Date: _____

How to Use This Checklist

For each statement, select the response that best reflects your current environment. Use the Notes column to record evidence, questions, or follow-up actions.

YES	PARTIAL	NO	N/A
Implemented and operating	Some elements exist	Not implemented / unknown	Not applicable

1. Governance & Accountability

Readiness statement	Yes	Partial	No	N/A	Notes
Cybersecurity responsibilities are formally assigned to an individual or team.	■	■	■	■	
Leadership receives periodic information about cybersecurity risk and priorities.	■	■	■	■	
Cybersecurity policies are documented, approved, communicated, and reviewed regularly.	■	■	■	■	
Technology and security risks are considered when making significant business decisions.	■	■	■	■	
Exceptions to security policies are documented, approved, and periodically reviewed.	■	■	■	■	

2. Asset & Risk Management

Readiness statement	Yes	Partial	No	N/A	Notes
The organization maintains an inventory of important hardware, software, cloud services, and information assets.	■	■	■	■	
Critical systems and data are identified based on business impact.	■	■	■	■	
Cybersecurity risk assessments are performed periodically and after significant changes.	■	■	■	■	
Known risks are documented, assigned an owner, and tracked through remediation or acceptance.	■	■	■	■	
Unsupported or end-of-life technology is identified and addressed through a replacement or mitigation plan.	■	■	■	■	

3. Identity & Access Management

Readiness statement	Yes	Partial	No	N/A	Notes
Each user has a unique account; shared accounts are limited and controlled.	■	■	■	■	
Multi-factor authentication is enabled for high-risk access such as email, remote access, cloud administration, and privileged accounts.	■	■	■	■	
Access is granted according to job responsibilities and least-privilege principles.	■	■	■	■	
User access is reviewed periodically and promptly removed when employment or responsibilities change.	■	■	■	■	
Privileged/administrator accounts are separated from normal day-to-day user accounts.	■	■	■	■	

4. Data Protection

Readiness statement	Yes	Partial	No	N/A	Notes
Sensitive and confidential information is identified and handled according to its level of sensitivity.	■	■	■	■	
Encryption is used for sensitive data when appropriate, including data in transit and at rest.	■	■	■	■	
Backups are performed regularly and protected from unauthorized modification or deletion.	■	■	■	■	
Backup restoration is tested periodically.	■	■	■	■	
Data retention and secure disposal practices are documented and followed.	■	■	■	■	

5. Endpoint, Network & Cloud Security

Readiness statement	Yes	Partial	No	N/A	Notes
Workstations, laptops, servers, and supported mobile devices receive security updates in a timely manner.	■	■	■	■	
Endpoint security/anti-malware protections are centrally managed where appropriate.	■	■	■	■	
Firewalls and network security controls are configured and reviewed.	■	■	■	■	
Remote access is protected using approved secure methods.	■	■	■	■	
Cloud services are configured using documented security standards and administrative access is restricted.	■	■	■	■	

6. Vulnerability & Patch Management

Readiness statement	Yes	Partial	No	N/A	Notes
The organization has a defined process for identifying vulnerabilities.	■	■	■	■	
Operating systems, applications, browsers, network devices, and security tools are patched according to risk and severity.	■	■	■	■	
Critical vulnerabilities are prioritized for timely remediation.	■	■	■	■	
Vulnerability findings are tracked until resolved, mitigated, or formally accepted.	■	■	■	■	
Internet-facing systems and services are reviewed regularly for unnecessary exposure.	■	■	■	■	

7. Security Awareness & Human Risk

Readiness statement	Yes	Partial	No	N/A	Notes
Personnel receive cybersecurity awareness training at hire and periodically thereafter.	■	■	■	■	
Users receive guidance on phishing, suspicious links, social engineering, and reporting security concerns.	■	■	■	■	
Security responsibilities for remote work and mobile devices are communicated.	■	■	■	■	
Personnel know how and where to report a suspected cybersecurity incident.	■	■	■	■	
Training completion is documented and monitored.	■	■	■	■	

8. Incident Response & Resilience

Readiness statement	Yes	Partial	No	N/A	Notes
A documented incident response plan identifies roles, responsibilities, communication paths, and escalation procedures.	■	■	■	■	
Important internal and external contacts are maintained for cybersecurity incidents.	■	■	■	■	
Incident response exercises or tabletop discussions are conducted periodically.	■	■	■	■	
Business continuity and recovery dependencies for critical systems are understood.	■	■	■	■	
Lessons learned from incidents or exercises are documented and used to improve controls.	■	■	■	■	

9. Third-Party & Vendor Risk

Readiness statement	Yes	Partial	No	N/A	Notes
Technology vendors and other third parties with access to systems or sensitive information are inventoried.	■	■	■	■	
Security and privacy requirements are considered before onboarding relevant vendors.	■	■	■	■	
Contracts address appropriate cybersecurity, confidentiality, incident notification, and data-handling expectations.	■	■	■	■	
High-risk vendors are periodically reviewed or reassessed.	■	■	■	■	
Vendor access is limited to what is necessary and removed when no longer required.	■	■	■	■	

10. Monitoring & Continuous Improvement

Readiness statement	Yes	Partial	No	N/A	Notes
Security events and alerts from important systems are reviewed by responsible personnel or a service provider.	■	■	■	■	
Significant security findings, incidents, and remediation activities are documented.	■	■	■	■	
Cybersecurity metrics or indicators are periodically reviewed by management.	■	■	■	■	
Policies, controls, and risk priorities are updated as the organization, threats, and technology change.	■	■	■	■	
Cybersecurity improvement activities are prioritized in a documented roadmap or action plan.	■	■	■	■	

Readiness Summary

Use this page to summarize the areas that need the most attention. A high number of "No" or "Partial" responses does not by itself determine risk; business impact, threat exposure, regulatory obligations, existing safeguards, and other context should also be considered.

Priority Area	Key Gap / Observation	Owner	Target Date
1.			
2.			
3.			
4.			
5.			

Suggested Next Steps

1. Review all Partial and No responses and identify which issues could materially affect operations, sensitive information, customers, or regulatory responsibilities.

2. Assign an accountable owner for each priority issue.

3. Develop realistic remediation actions with target dates and required resources.

4. Track progress and reassess readiness periodically and after significant technology or organizational changes.

Need a deeper assessment?
CTRL The Future LLC provides advisory support for cybersecurity risk, governance, compliance, and technology strategy. A formal engagement can include evidence review, risk analysis, gap assessment, prioritized recommendations, and a practical improvement roadmap.

Disclaimer: This checklist is provided for general informational and readiness purposes only. It does not constitute legal advice, regulatory certification, a guarantee of security, or a complete cybersecurity risk assessment. Organizations should evaluate requirements applicable to their specific environment and circumstances.