CONNECTING PEOPLE AND INFORMATION TO THE WORLD – SECURELY

CYBER ESSENTIALS CHECKLIST

A simple guide to spot gaps, choose priorities, and strengthen everyday cybersecurity.

Who it is for: Any organization that wants a clearer cybersecurity baseline.

How to use it: Review it together, choose the biggest gaps, assign owners, and check back quarterly.

VECTORUSA
CYBERSECURITY SERVICES

Tel: 800.929.4516 | Web: www.vectorusa.com

SECURITY POSTURE REVIEW

Not sure how to score something? Start here. Turn unclear answers into action items.

Ownership and priorities

- Who owns cybersecurity decisions?
- Which systems would hurt the organization most if they went down?
- What risks are clear today? What is still unknown?

Identity and access

- Where is MFA missing?
- How often are admin and inactive accounts reviewed?
- Are shared and service accounts documented?

Monitoring and response

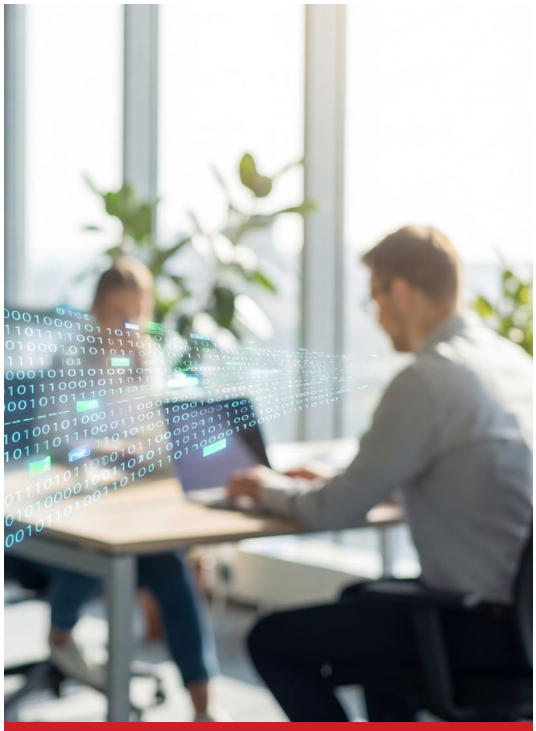
- Who reviews alerts at night or on weekends?
- Which alerts matter? Which are noise?
- How quickly can the team contain an issue?

Recovery

- When was the last successful restore test?
- Can backups be deleted or changed by ransomware or an unauthorized user?
- Does the response plan include key internal and external contacts?

People and training

- Do people know how to report suspicious activity?
- Does training match the risks people face?
- Is training reinforced throughout the year?



"Organizations need experienced cybersecurity professionals who can identify real threats, investigate suspicious activity, and respond quickly when every minute matters,"

- William Higgins, VP of Information Systems

Priority Notes

HOW TO USE THIS CHECKLIST

Use this checklist to identify security gaps, clarify ownership, and prioritize practical next steps.

1. **Review each question**
   Consider your organization's current practices, not what is planned or assumed.
2. **Select a score from 0 to 3**
   Choose the response that most accurately reflects what is in place today.
3. **Add context**
   Document unclear answers, known gaps, supporting evidence, or questions requiring follow-up.
4. **Prioritize action**
   Focus first on items scored 0 or 1, especially those affecting critical systems, sensitive data, recovery, or incident response.
5. **Assign accountability**
   Give each priority item an owner, target date, and clear next step.
6. **Review regularly**
   Revisit the checklist at least quarterly and after major technology, staffing, vendor, or business changes.

Readiness Scoring Guide

0	Not started	Not in place or no clear owner.	**FIX FIRST**
1	In progress	Partly in place or inconsistent.	**NEXT**
2	In place	Defined, owned, and working.	**MAINTAIN**
3	Managed	Reviewed, tested, and improved.	**IMPROVE**

Quick guide: Scores of 0 or 1 need action. Scores of 2 or 3 still need regular review and testing.

Checklist Summary

Total Score	Readiness	What to focus on
0 to 14	High priority	Start with access, backups, patching, and response.
15 to 28	Making progress	Close gaps, document the basics, and test what is in place.
29 to 42	Strong foundation	Keep testing, improving, and sharing progress.

CYBER ESSENTIALS CHECKLIST

Give each item a score from 0 to 3. Add an owner for anything that needs work.

0-3	Area	What to check	Owner
☐	Governance and ownership	A leader owns cybersecurity. Policies, key risks, and review dates are documented.	
☐	Asset inventory	Devices, apps, cloud services, data, and critical systems are listed and kept current.	
☐	Identity and access	Multi-factor authentication (MFA) covers email, remote access, admin, and cloud accounts. Access is reviewed.	
☐	Secure configuration	Systems use secure settings. Default passwords, unused accounts, and unused services are removed.	
☐	Patch management	Critical updates are tracked and installed on time.	
☐	Endpoint protection	Devices have current endpoint protection. Alerts are reviewed and escalated.	
☐	Email and web protection	Email, phishing, web, and domain protections are turned on and monitored.	
☐	Data protection	Sensitive data is identified, limited to the right people, protected, and deleted when no longer needed.	
☐	Backup and recovery	Backups run automatically, are protected, stored separately, and tested.	
☐	Logging and monitoring	Key systems send logs to one place. Important events are reviewed and escalated.	
☐	Incident response	A current response plan names contacts, decisions, and next steps. The plan is practiced.	
☐	Security awareness	People get practical training and know how to report suspicious activity.	
☐	Vendor risk	Critical vendors are tracked, have security expectations, and are included in response plans.	
☐	Compliance and reporting	Security work is documented for leader ship, insurance, audits, customers, or other requirements.	

Enter one score from 0 to 3 in each box. The total updates automatically on page 5.

YOUR SCORE

TOTAL SCORE	0	/ 42

0-14	15-28	29-42
HIGH PRIORITY	MAKING PROGRESS	STRONG FOUNDATION

Next Step

Talk with VectorUSA about a cybersecurity readiness review. We will help identify priorities, check current controls, and build a practical plan.

A cybersecurity readiness review may help if:

- You are not sure which systems or risks matter most.
- Alerts are not reviewed consistently or ownership is unclear.
- MFA, patching, backups, or endpoint protection are incomplete.
- Leadership, insurers, auditors, or customers need clearer reporting.
- Your team needs a practical plan and extra support.

Keep the plan focused on a few changes that reduce the most risk.

First 30 Days: Fix the basics

- Confirm the owner and decision makers.
- Close priority MFA, patching, and backup gaps.
- List critical systems and services.
- Update the incident contact list.

Days 31 to 60: Improve visibility

- Centralize logs for key systems.
- Review endpoint and email protection.
- Tighten onboarding, offboarding, and access reviews.
- Run a short incident practice session.

Days 61 to 90: Test and report

- Test a restore and document the result.
- Track response times, open gaps, and repeat alerts.
- Share progress, remaining risk, and budget needs.
- Schedule the next quarterly review.

FOR MORE INFO:
Visit www.vectorusa.com
800.929.4516

Or scan the code.