Asili Advisory Group: Cybersecurity Readiness Checklist

	YES	NO

1. Authentication & Access Control:

If a cybercriminal tried to access our systems today, would our authentication stop them and do our access controls limit damage if they got in?

All critical business accounts use multi-factor authentication	☐	☐
We use strong, unique passwords managed by a business password manager	☐	☐
Employee access is reviewed and updated when roles change	☐	☐
We control and regularly audit who has administrative system access	☐	☐

2. Employee Security Awareness:

Could our team spot and stop a cyberattack, and do our security practices prove we take it seriously (showing we're prepared)?

Our team can confidently identify phishing emails and suspicious links	☐	☐
Employees know exactly who to contact about suspicious activity	☐	☐
We regularly train staff on current cybersecurity threats and best practices	☐	☐

3. Security Culture:

If our IT person left tomorrow, would we still feel cyber-ready?

Cybersecurity isn't just the IT person's job – everyone plays a part	☐	☐
Leaders, managers, and staff all help build security confidence	☐	☐
We set high expectations for security across the whole organization	☐	☐

4. Backup & Recovery:

When was the last time we successfully tested restoring our critical data?

We regularly test our backups to ensure they actually work when needed	☐	☐
Our backup systems are protected from ransomware attacks	☐	☐
We can restore critical systems within 4 hours of a failure	☐	☐
Our recovery procedures are documented and everyone knows their role	☐	☐

5. Systems & Software Security:

Could a cybercriminal get us from one glance at our network security?

All software and systems receive security updates within 48 hours	☐	☐
We have endpoint protection on all devices accessing business data	☐	☐
Our network is properly configured, secured, and monitored	☐	☐
We regularly scan for vulnerabilities in our systems and applications	☐	☐

6. Incident Response & Compliance:

Would a cybercriminal looking at our response capabilities feel confident we're prepared, professional, and compliant and is our security approach consistent with our business strategy?

- [ ] We have written cybersecurity policies that employees actually follow
- [ ] We know exactly what to do if we discover a security breach
- [ ] Our cybersecurity meets industry and regulatory requirements
- [ ] We have appropriate cyber insurance and understand what it covers
- [ ] We document security incidents and use them to improve our defenses

Complete this assessment to identify your cybersecurity gaps.
Contact Asili for professional evaluation and implementation support.
info@asiliadvisors.com