Security Self-Assessment

Cybercriminals, empowered by AI, are more **organized**, **disciplined**, and **persistent** than ever. This means that our cybersecurity strategies must rise to meet the evolving challenge, and controls that we used to view as "advanced" measures must now become our baseline.

To help benchmark your current security posture, we've compiled the following checklist. Please keep in mind that this is a partial list, **not** a substitute for a formal strategy or compliance framework.

EMAIL & OFFICE 365

- [ ] External emails have warning banner
- [ ] Multi-factor authentication is required
- [ ] SafeLinks scan for malicious URLs
- [ ] Conditional access policies restrict sign-ins

AWARENESS TRAINING

- [ ] Employees are trained annually
- [ ] Phishing tests are regularly simulated
- [ ] Regular micro-trainings are delivered

ENDPOINT SECURITY

- [ ] All devices have AI threat detection
- [ ] Computers and mobile devices are encrypted
- [ ] VPN is in use and enforced during travel
- [ ] Employees do not have local admin rights

DATA GOVERNANCE

- [ ] File sharing defaults are NOT "anyone"
- [ ] Data is backed up offsite
- [ ] Data retention is controlled and documented
- [ ] Employees use a central password manager

APPLICATION CONTROL

- [ ] Application allowlisting is enforced
- [ ] Single Sign-On is enforced where available
- [ ] Audit process is documented and followed

POLICIES

- [ ] Data & Folder Naming Conventions
- [ ] Unsupported Software & App Request
- [ ] Acceptable Use & Security Training
- [ ] Incident Response

We also recommend allocating a **dedicated budget line for cybersecurity**, rather than assuming it is fully covered under your general IT expenses. This line can encompass periodic assessments, remediation projects, supplemental defenses, and more.

Finally, even if you aren't subject to compliance regulations, **pick a security framework** to give structure to your approach. NIST 800-171 is a good option for those without specific requirements.