CHECKLIST INTELLIGENT iT CYBERSECURITY

Cybersecurity Risk Assessment Checklist

20 critical controls every business should evaluate to reduce cyber risk.

Use this checklist to audit your organization's security posture. Each item maps to industry frameworks (NIST, CIS Controls). Check off completed items and prioritize gaps.

IDENTITY & ACCESS MANAGEMENT

- [ ] Multi-factor authentication (MFA) enforced on all user accounts and admin portals
- [ ] Role-based access control (RBAC) implemented with least-privilege policies
- [ ] Privileged accounts inventoried, monitored, and rotated on a regular schedule
- [ ] Single sign-on (SSO) deployed across all business-critical applications

ENDPOINT & NETWORK SECURITY

- [ ] Endpoint Detection & Response (EDR) deployed on all workstations and servers
- [ ] Next-gen firewall configured with intrusion prevention enabled
- [ ] DNS filtering active to block malicious domains
- [ ] Automatic OS and software patching within 14 days of release
- [ ] Mobile Device Management (MDM) enforced on all company and BYOD devices

EMAIL & PHISHING

- [ ] Email filtering with anti-phishing, anti-malware, and sandboxing enabled
- [ ] DMARC, DKIM, and SPF records configured for all company domains
- [ ] Phishing simulation training conducted quarterly for all employees

DATA PROTECTION & BACKUP

- [ ] Critical data backed up daily with 3-2-1 strategy (3 copies, 2 media, 1 offsite)
- [ ] Backup restoration tested quarterly with documented results
- [ ] Data Loss Prevention (DLP) policies configured for sensitive data
- [ ] Full-disk encryption enabled on all laptops and portable storage

INCIDENT RESPONSE & GOVERNANCE

- [ ] Documented incident response plan reviewed and updated annually
- [ ] Security awareness training completed by all employees at least annually
- [ ] Vulnerability scanning performed monthly; penetration testing annually

- [ ] Cyber insurance policy active and reviewed with current risk profile