CLOUDAVIZE

Cybersecurity Checklist

Cybersecurity Governance and Policies :

- [ ] Is there a documented cybersecurity strategy aligned with business objectives?
- [ ] Are cybersecurity policies and procedures in place, comprehensive, and up-to-date?
- [ ] Is there a designated cybersecurity team or individual responsible for cybersecurity?
- [ ] Is cybersecurity risk management integrated into overall business risk management?
- [ ] Is cybersecurity awareness training provided to all employees regularly?

Security Controls and Technologies :

- [ ] Are firewalls and intrusion detection/prevention systems (IDS/IPS) implemented and configured correctly?
- [ ] Is anti-malware software deployed and updated on all endpoints?
- [ ] Is vulnerability management process in place (scanning, patching, penetration testing)?
- [ ] Are access controls and strong password policies enforced?
- [ ] Is multi-factor authentication (MFA) implemented for critical systems and accounts?
- [ ] Is data encryption used for sensitive data at rest and in transit?
- [ ] Is endpoint detection and response (EDR) solution implemented?
- [ ] Is Security Information and Event Management (SIEM) system used for security monitoring?

Incident Response and Recovery :

- [ ] Is there a documented incident response plan (IRP)?
- [ ] Are incident response procedures tested and practiced regularly?
- [ ] Is there an incident response team with defined roles and responsibilities?
- [ ] Are backup and recovery procedures in place and tested?
- [ ] Is there a disaster recovery plan (DRP) and business continuity plan (BCP)?

Network and Infrastructure Security :

- [ ] Is network segmentation implemented to isolate critical systems?
- [ ] Is wireless network security properly configured (e.g., WPA3)?
- [ ] Is VPN access used for secure remote access?
- [ ] Are network devices and systems hardened and securely configured?

Data Security and Privacy :

- [ ] Are data classification and data loss prevention (DLP) measures implemented?
- [ ] Are data privacy regulations (e.g., GDPR, CCPA) addressed?
- [ ] Are data retention and deletion policies defined and enforced?
- [ ] Is data access audited and monitored?

Third-Party and Supply Chain Security :

- [ ] Are third-party vendors and suppliers assessed for cybersecurity risks?
- [ ] Are security requirements included in contracts with third parties?
- [ ] Is supply chain security risk management implemented?

Emerging Threats and Technologies :

- [ ] Is the organization aware of emerging cybersecurity threats and trends?
- [ ] Are new technologies and security solutions evaluated and adopted as needed?
- [ ] Is threat intelligence used to proactively identify and mitigate threats?

You can find this checklist at

https://www.cloudavize.com/cybersecurity-checklist