CLOUDAVIZE

IT Security Audit Checklist

✓ Security Policies and Procedures :

□ Are security policies and procedures documented, comprehensive, and up-to-date?
□ Are security policies communicated to all employees and users?
□ Are there policies covering acceptable use, password management, data security, incident response, etc.?
□ Are policies regularly reviewed and updated to reflect current threats and best practices?

✓ Access Control and Identity Management :

□ Are access controls implemented based on the principle of least privilege?
□ Are user accounts managed and monitored effectively?
□ Are strong password policies enforced (complexity, length, rotation)?
□ Is multi-factor authentication (MFA) implemented for critical systems and accounts?
□ Are privileged access management (PAM) controls in place for administrative accounts?
□ Are access rights reviewed and revoked when employees leave or change roles (offboarding process)?

✓ Network Security : (See also dedicated Network Security Checklist)

□ Are firewalls properly configured and maintained at network boundaries?
□ Is intrusion detection/prevention system (IDS/IPS) implemented and monitored?
□ Is network segmentation implemented to isolate critical systems and data?
□ Is wireless network security properly configured (e.g., WPA3 encryption)?
□ Is VPN access used for secure remote access?
□ Are network vulnerabilities regularly scanned and remediated?

✓ Endpoint Security : (See also dedicated Endpoint Security Audit Checklist)

□ Is anti-malware software deployed and updated on all endpoints (desktops, laptops, servers)?
□ Are endpoint detection and response (EDR) solutions implemented?
□ Are operating systems and applications patched regularly?
□ Is full disk encryption enabled on laptops and portable devices?
□ Are endpoint security policies enforced (e.g., USB device control, application whitelisting)?

✓ Vulnerability Management :

□ Are regular vulnerability scans performed on systems and applications?
□ Are vulnerabilities prioritized and remediated in a timely manner?
□ Is penetration testing conducted periodically to assess security posture?
□ Is there a process for tracking and managing vulnerabilities?

✓ Incident Response :

- □ Is there a documented incident response plan (IRP)?
- □ Are incident response procedures tested and practiced?
- □ Is there an incident response team with defined roles and responsibilities?
- □ Are security incidents logged, investigated, and reported?
- □ Are lessons learned from incidents used to improve security controls?

✓ Physical Security :

- □ Are physical access controls in place for server rooms and data centers (e.g., access cards, security cameras)?
- □ Are environmental controls in place to protect IT equipment (temperature, humidity, power)?

✓ Security Awareness Training :

- □ Is security awareness training provided to all employees regularly?
- □ Does training cover topics like phishing, social engineering, password security, and data protection?
- □ Is the effectiveness of security awareness training measured?

You can find this checklist at

https://www.cloudavize.com/it-security-audit-checklist