

## IT Audit Checklist

### Network & Infrastructure

Section	Checklist Items
<input type="checkbox"/> Firewall	We check the firewall to determine if it's properly configured, regularly updated and secured (i.e., security services enabled?) to prevent unauthorized access and data breaches. The lack of a properly configured firewall is a common entry point for cyberattacks.
<input type="checkbox"/> Wi-Fi Security	We check for strong Wi-Fi encryption (WPA2/3) and proper network segmentation (e.g., separating guest networks from internal resources) to prevent unauthorized access and potential attacks.
<input type="checkbox"/> Server Room	We check for proper physical security, cooling, and power backups to prevent downtime, overheating, and unauthorized access to critical IT assets.

### Endpoint & Device Security

Section	Checklist Items
<input type="checkbox"/> Computers	We check that operating systems are regularly updated, antivirus software is installed, and data encryption is enabled to protect endpoints from malware, data theft, and unauthorized access.
<input type="checkbox"/> Patch Management	We check that all systems receive timely updates and patches to reduce vulnerabilities that attackers could exploit.
<input type="checkbox"/> Unauthorized Devices	We check for unauthorized or unknown devices on the network to prevent security risks such as data leaks and insider threats.

### Data Security & Backup

Section	Checklist Items
<input type="checkbox"/> Access Controls	We check that role-based access controls (RBAC) are enforced to ensure employees only have the minimum permissions required for their roles, reducing insider threats and accidental data exposure.
<input type="checkbox"/> Data Encryption	We check that sensitive data is encrypted both at rest and in transit to protect it from being intercepted or stolen in the event of a breach.
<input type="checkbox"/> Backup	We check that regular backups are performed and tested to ensure critical business data can be restored in case of ransomware attacks, hardware failures, or accidental deletions.

### Cloud & SaaS Security

Section	Checklist Items
<input type="checkbox"/> Multi-Factor Authentication	We check that Identity and Access Management (IAM) controls and Multi-Factor Authentication (MFA) are in place to reduce the risk of unauthorized account access, especially for cloud-based services.
<input type="checkbox"/> Cloud & SaaS Security	We check that cloud security settings are properly configured and that unauthorized SaaS applications (Shadow IT) are monitored to maintain compliance and prevent data leaks.

### Physical Security

Section	Checklist Items
<input type="checkbox"/> Physical Security	We check that physical access to critical IT infrastructure is restricted and monitored to prevent unauthorized tampering, theft, and physical breaches.

### Security Policies & Awareness

Section	Checklist Items
<input type="checkbox"/> Incident Response Plan	We check that a documented and tested incident response plan is in place to ensure quick and effective action in case of cyberattacks or security breaches.
<input type="checkbox"/> Security Awareness	We check that employees receive regular security awareness training on phishing attacks, social engineering, and password hygiene to reduce the risk of human error leading to breaches.
<input type="checkbox"/> Compliance	We check that IT security practices align with industry standards (ISO 27001, NIST, HIPAA, etc.) to protect against legal and financial risks while ensuring best security practices.