It Security Audit Checklist

Free It Security Audit Checklist with AI customization. Industry-specific guidance for it security audit checklist. Build your checklist now.

Security Governance

- [ ] Security strategy documented
- [ ] Policies comprehensive and current
- [ ] Standards defined and enforced
- [ ] Procedures detailed
- [ ] Guidelines available
- [ ] Roles/responsibilities clear
- [ ] Security organization structured
- [ ] Reporting lines established
- [ ] Budget adequate
- [ ] Metrics defined
- [ ] Performance measured
- [ ] Improvement continuous

Access Control Management

- [ ] Access control policy enforced
- [ ] User registration controlled
- [ ] User access provisioning managed
- [ ] Privileged access restricted
- [ ] Access rights reviewed regularly
- [ ] Password management enforced
- [ ] Multi-factor authentication deployed
- [ ] Single sign-on implemented
- [ ] Account lockout configured
- [ ] Inactive accounts disabled
- [ ] Service accounts secured
- [ ] Emergency access controlled

Network Security

- [ ] Network architecture secure
- [ ] Segmentation implemented
- [ ] Firewalls configured properly
- [ ] IDS/IPS operational
- [ ] VPN access controlled
- [ ] Wireless security enforced
- [ ] Remote access secured
- [ ] Network monitoring active

- [ ] Traffic analysis performed
- [ ] Vulnerability scanning regular
- [ ] Penetration testing conducted
- [ ] Patch management current

Data Protection

- [ ] Data classification implemented
- [ ] Encryption standards enforced
- [ ] Data at rest protected
- [ ] Data in transit secured
- [ ] Key management robust
- [ ] Data loss prevention active
- [ ] Backup procedures verified
- [ ] Recovery capability tested
- [ ] Retention policies followed
- [ ] Disposal procedures secure
- [ ] Privacy controls implemented
- [ ] Compliance maintained

Application Security

- [ ] Secure coding standards followed
- [ ] Security requirements defined
- [ ] Threat modeling performed
- [ ] Security testing conducted
- [ ] Code reviews performed
- [ ] Vulnerability assessments done
- [ ] Web application firewalls deployed
- [ ] API security implemented
- [ ] Database security configured
- [ ] Input validation enforced
- [ ] Output encoding implemented
- [ ] Session management secure

Endpoint Security

- [ ] Endpoint protection deployed
- [ ] Antivirus/antimalware current
- [ ] Host firewalls enabled
- [ ] Patch management automated
- [ ] Configuration standards enforced
- [ ] Mobile device management active
- [ ] Encryption enforced
- [ ] USB controls implemented
- [ ] Application whitelisting used
- [ ] Browser security configured
- [ ] Email security enabled

- [ ] Asset inventory maintained

Identity Management

- [ ] Identity lifecycle managed
- [ ] Authentication mechanisms strong
- [ ] Authorization properly configured
- [ ] Federation implemented
- [ ] Directory services secured
- [ ] Privileged identity managed
- [ ] Service accounts controlled
- [ ] API keys secured
- [ ] Certificates managed
- [ ] Biometrics implemented appropriately
- [ ] Identity governance active
- [ ] Compliance maintained

Security Operations

- [ ] SOC operational
- [ ] 24/7 monitoring active
- [ ] Log collection comprehensive
- [ ] SIEM configured effectively
- [ ] Correlation rules tuned
- [ ] Threat intelligence integrated
- [ ] Incident detection timely
- [ ] Alert management efficient
- [ ] Forensics capability ready
- [ ] Threat hunting performed
- [ ] Metrics tracked
- [ ] Reporting effective

Incident Response

- [ ] IR plan documented and current
- [ ] IR team trained and ready
- [ ] Roles/responsibilities defined
- [ ] Contact information current
- [ ] Detection capabilities adequate
- [ ] Containment procedures ready
- [ ] Eradication processes defined
- [ ] Recovery procedures tested
- [ ] Communication plan ready
- [ ] Evidence preservation understood
- [ ] Lessons learned captured
- [ ] Improvements implemented

Physical Security

- [ ] Physical access controlled
- [ ] Data center security adequate
- [ ] Server room access restricted
- [ ] Visitor management enforced
- [ ] Surveillance systems operational
- [ ] Environmental controls working
- [ ] Equipment disposal secure
- [ ] Media handling controlled
- [ ] Clean desk policy enforced
- [ ] Printing controlled
- [ ] Key management secure
- [ ] Perimeter security effective

Third-Party Security

- [ ] Vendor risk assessed
- [ ] Security requirements contractual
- [ ] Due diligence performed
- [ ] Ongoing monitoring active
- [ ] Access strictly controlled
- [ ] Data protection enforced
- [ ] Incident notification required
- [ ] Compliance verified
- [ ] Performance monitored
- [ ] Audits conducted
- [ ] Issues remediated
- [ ] Relationships managed

Compliance & Audit

- [ ] Regulatory requirements identified
- [ ] Compliance framework implemented
- [ ] Controls mapped
- [ ] Testing performed regularly
- [ ] Evidence collected
- [ ] Gaps identified and closed
- [ ] Audit program active
- [ ] Findings tracked
- [ ] Remediation timely
- [ ] Certifications maintained
- [ ] Reporting accurate
- [ ] Continuous improvement shown