Cyber Security Audit Checklist

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

Network Security

- [ ] Firewall configurations reviewed
- [ ] Intrusion detection active
- [ ] Intrusion prevention enabled
- [ ] Network segmentation proper
- [ ] DMZ properly configured
- [ ] VPN security adequate
- [ ] Wireless security enforced
- [ ] Network monitoring active
- [ ] Traffic analysis performed
- [ ] Anomaly detection working
- [ ] DDoS protection enabled
- [ ] Network documentation current

Access Control

- [ ] Identity management system active
- [ ] Multi-factor authentication enabled
- [ ] Privileged access managed
- [ ] Role-based access implemented
- [ ] Least privilege enforced
- [ ] Access reviews conducted
- [ ] Terminated user cleanup done
- [ ] Service accounts secured
- [ ] Password policies enforced
- [ ] Account lockout configured
- [ ] Session management proper
- [ ] Remote access secured

Data Protection

- [ ] Data classification implemented
- [ ] Encryption at rest enabled
- [ ] Encryption in transit enforced
- [ ] Key management secure
- [ ] Data loss prevention active
- [ ] Backup procedures tested
- [ ] Recovery procedures verified
- [ ] Data retention followed

- [ ] Secure disposal practiced
- [ ] Database security configured
- [ ] File integrity monitoring
- [ ] Data masking implemented

Endpoint Security

- [ ] Antivirus/anti-malware current
- [ ] Endpoint detection active
- [ ] Host firewall enabled
- [ ] Patch management current
- [ ] Configuration management enforced
- [ ] Mobile device management
- [ ] Removable media controlled
- [ ] Application whitelisting used
- [ ] Browser security configured
- [ ] Email security enabled
- [ ] Disk encryption active
- [ ] Asset inventory maintained

Application Security

- [ ] Secure coding practices followed
- [ ] Code reviews conducted
- [ ] Static analysis performed
- [ ] Dynamic testing done
- [ ] Vulnerability scanning regular
- [ ] Penetration testing performed
- [ ] OWASP standards followed
- [ ] Input validation implemented
- [ ] Authentication secure
- [ ] Authorization proper
- [ ] Session management secure
- [ ] API security implemented

Cloud Security

- [ ] Cloud architecture reviewed
- [ ] Identity federation configured
- [ ] Cloud access broker used
- [ ] Container security implemented
- [ ] Serverless security addressed
- [ ] Cloud storage encrypted
- [ ] Cloud monitoring active
- [ ] Cloud compliance verified
- [ ] SaaS security configured
- [ ] IaaS/PaaS security proper
- [ ] Multi-cloud security managed

- [ ] Cloud backup verified

Incident Response

- [ ] Incident response plan current
- [ ] Response team identified
- [ ] Contact list updated
- [ ] Detection capabilities tested
- [ ] Containment procedures ready
- [ ] Eradication processes defined
- [ ] Recovery procedures documented
- [ ] Lessons learned captured
- [ ] Forensics capability available
- [ ] Evidence preservation procedures
- [ ] Communication plan ready
- [ ] Legal requirements understood

Security Awareness

- [ ] Training program active
- [ ] Phishing simulations conducted
- [ ] Security policies communicated
- [ ] Awareness materials distributed
- [ ] Metrics tracked
- [ ] High-risk groups targeted
- [ ] Executive training provided
- [ ] Vendor training required
- [ ] Onboarding includes security
- [ ] Annual refresher mandatory
- [ ] Incident reporting encouraged
- [ ] Security culture promoted

Vulnerability Management

- [ ] Vulnerability scanning regular
- [ ] Patch management process defined
- [ ] Critical patches prioritized
- [ ] Testing procedures followed
- [ ] Emergency patching ready
- [ ] Third-party patches included
- [ ] Firmware updates managed
- [ ] Configuration vulnerabilities addressed
- [ ] Risk scoring implemented
- [ ] Remediation tracked
- [ ] Exceptions documented
- [ ] Metrics reported

Physical Security

- [ ] Data center security adequate
- [ ] Access controls enforced
- [ ] Visitor management proper
- [ ] Security cameras operational
- [ ] Environmental controls working
- [ ] Equipment disposal secure
- [ ] Clean desk policy enforced
- [ ] Printing controls implemented
- [ ] Physical key management
- [ ] Facility monitoring active
- [ ] Security guards effective
- [ ] Emergency response ready

Third-Party Risk

- [ ] Vendor assessments conducted
- [ ] Security requirements defined
- [ ] Contracts include security
- [ ] Right to audit included
- [ ] Incident notification required
- [ ] Data handling specified
- [ ] Compliance verified
- [ ] Risk ratings assigned
- [ ] Monitoring ongoing
- [ ] Performance measured
- [ ] Issues remediated
- [ ] Termination procedures defined

Compliance & Governance

- [ ] Security policies comprehensive
- [ ] Standards documented
- [ ] Procedures detailed
- [ ] Roles defined clearly
- [ ] Responsibilities assigned
- [ ] Governance structure effective
- [ ] Risk management mature
- [ ] Compliance frameworks followed
- [ ] Audit findings addressed
- [ ] Metrics tracked
- [ ] Board reporting done
- [ ] Continuous improvement active