WriteVoice.io - Talk, don't type. It's 4x faster.

Cybersecurity Audit Checklist

Free Cybersecurity Audit Checklist with AI customization. Industry-specific guidance for cybersecurity audit checklist. Build your checklist now.

Security Governance

- [ ] Information security policy documented
- [ ] Security roles and responsibilities defined
- [ ] Security awareness program active
- [ ] Risk management framework implemented
- [ ] Security metrics and KPIs tracked
- [ ] Board reporting on security
- [ ] Budget allocation appropriate
- [ ] Third-party risk management
- [ ] Incident response plan tested
- [ ] Business continuity planning
- [ ] Compliance framework maintained
- [ ] Security architecture documented

Identity & Access Management

- [ ] Identity governance implemented
- [ ] Privileged access management (PAM)
- [ ] Multi-factor authentication (MFA) enforced
- [ ] Single sign-on (SSO) deployed
- [ ] Password policies enforced
- [ ] Account lifecycle management
- [ ] Access certification regular
- [ ] Segregation of duties maintained
- [ ] Service account management
- [ ] Remote access controls
- [ ] Guest/contractor access managed
- [ ] Access logging and monitoring

Network Security

- [ ] Network segmentation implemented
- [ ] Firewall rules documented/tested
- [ ] Intrusion detection/prevention (IDS/IPS)
- [ ] Virtual private network (VPN) secure
- [ ] Wireless security WPA3/enterprise
- [ ] Network access control (NAC)
- [ ] DNS security (DNSSEC)
- [ ] DDoS protection active

- [ ] Load balancer security
- [ ] Certificate management
- [ ] Network monitoring 24/7
- [ ] Traffic analysis performed

Endpoint Protection

- [ ] Antivirus/anti-malware deployed
- [ ] Endpoint detection & response (EDR)
- [ ] Host-based firewall enabled
- [ ] Application whitelisting
- [ ] Device encryption enforced
- [ ] Mobile device management (MDM)
- [ ] Patch management automated
- [ ] USB/removable media controls
- [ ] Screen lock policies
- [ ] Remote wipe capability
- [ ] Asset inventory current
- [ ] Configuration management

Data Security

- [ ] Data classification scheme
- [ ] Data loss prevention (DLP) tools
- [ ] Encryption at rest implemented
- [ ] Encryption in transit enforced
- [ ] Key management procedures
- [ ] Database security controls
- [ ] Backup encryption verified
- [ ] Data retention policies
- [ ] Secure data disposal
- [ ] Data masking/tokenization
- [ ] Rights management (DRM)
- [ ] Privacy controls implemented

Application Security

- [ ] Secure SDLC implemented
- [ ] Code reviews conducted
- [ ] Static analysis (SAST) performed
- [ ] Dynamic testing (DAST) done
- [ ] Dependency scanning active
- [ ] Web application firewall (WAF)
- [ ] API security controls
- [ ] Container security scanning
- [ ] Secrets management solution
- [ ] Input validation enforced
- [ ] Session management secure

- [ ] Security testing automated

Cloud Security

- [ ] Cloud security architecture
- [ ] Cloud access security broker (CASB)
- [ ] Cloud workload protection (CWPP)
- [ ] Cloud security posture management (CSPM)
- [ ] Identity federation configured
- [ ] Cloud encryption enabled
- [ ] Cloud backup verified
- [ ] Multi-cloud security
- [ ] Serverless security controls
- [ ] Container orchestration security
- [ ] Cloud compliance monitoring
- [ ] Cloud incident response

Security Operations

- [ ] Security operations center (SOC)
- [ ] SIEM platform operational
- [ ] Log collection comprehensive
- [ ] Correlation rules effective
- [ ] Threat intelligence integrated
- [ ] Incident tickets tracked
- [ ] Forensics capability ready
- [ ] Threat hunting performed
- [ ] Security orchestration (SOAR)
- [ ] Metrics and reporting
- [ ] 24/7 monitoring coverage
- [ ] Escalation procedures defined

Vulnerability Management

- [ ] Vulnerability scanning scheduled
- [ ] Authenticated scanning performed
- [ ] External scanning conducted
- [ ] Web application scanning
- [ ] Database scanning included
- [ ] Cloud infrastructure scanning
- [ ] Penetration testing annual
- [ ] Red team exercises conducted
- [ ] Bug bounty program active
- [ ] Patch management process
- [ ] Risk scoring methodology
- [ ] Remediation SLAs defined

Physical Security

- [ ] Physical access controls
- [ ] Badge system management
- [ ] Visitor management procedures
- [ ] Security cameras operational
- [ ] Security guard coverage
- [ ] Data center security
- [ ] Environmental monitoring
- [ ] Clean desk policy
- [ ] Document disposal secure
- [ ] Equipment disposal procedures
- [ ] Lock and key management
- [ ] Perimeter security adequate

Incident Response

- [ ] Incident response team defined
- [ ] Response procedures documented
- [ ] Classification scheme clear
- [ ] Communication plan ready
- [ ] Containment strategies defined
- [ ] Eradication procedures ready
- [ ] Recovery plans tested
- [ ] Evidence preservation procedures
- [ ] Legal counsel identified
- [ ] PR/communications ready
- [ ] Lessons learned process
- [ ] Tabletop exercises conducted

Compliance & Audit

- [ ] Regulatory requirements mapped
- [ ] Compliance monitoring active
- [ ] Audit schedule maintained
- [ ] Control testing performed
- [ ] Evidence collection organized
- [ ] Gap assessments conducted
- [ ] Remediation tracked
- [ ] Certification maintained
- [ ] External audits supported
- [ ] Internal audits regular
- [ ] Policy exceptions tracked
- [ ] Continuous improvement program

By WriteVoice.io - Talk, don't type. It's 4x faster