Security Audit Checklist

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

Physical Security

- [ ] Perimeter security adequate
- [ ] Access control systems functional
- [ ] Badge system properly managed
- [ ] Visitor management procedures followed
- [ ] Security cameras operational and recording
- [ ] Lighting sufficient in all areas
- [ ] Alarm systems tested regularly
- [ ] Guard services effective
- [ ] Key management controlled
- [ ] Secure areas properly restricted
- [ ] Loading dock procedures enforced
- [ ] Emergency exits accessible but secure

Information Security Policy

- [ ] Security policy comprehensive and current
- [ ] Standards documented and communicated
- [ ] Procedures detailed and followed
- [ ] Guidelines available and understood
- [ ] Roles and responsibilities defined
- [ ] Enforcement mechanisms in place
- [ ] Exception process documented
- [ ] Review cycle established
- [ ] Training requirements specified
- [ ] Compliance monitoring active
- [ ] Violation consequences clear
- [ ] Management support evident

Access Control

- [ ] User provisioning process controlled
- [ ] Identity verification performed
- [ ] Authorization properly granted
- [ ] Privileged access managed strictly
- [ ] Password policies enforced
- [ ] Multi-factor authentication deployed
- [ ] Account reviews conducted regularly
- [ ] Terminated access removed promptly

- [ ] Service accounts inventoried
- [ ] Generic accounts eliminated
- [ ] Guest access controlled
- [ ] Remote access secured

Network Security

- [ ] Firewall configurations reviewed
- [ ] Rules documented and justified
- [ ] Segmentation implemented properly
- [ ] DMZ configured correctly
- [ ] Intrusion detection active
- [ ] Intrusion prevention enabled
- [ ] VPN access controlled
- [ ] Wireless networks secured
- [ ] Network monitoring continuous
- [ ] Vulnerability scanning regular
- [ ] Penetration testing performed
- [ ] Patch management current

Data Protection

- [ ] Data classification implemented
- [ ] Sensitive data identified
- [ ] Encryption requirements defined
- [ ] Encryption properly implemented
- [ ] Key management procedures secure
- [ ] Data loss prevention active
- [ ] Backup procedures verified
- [ ] Recovery testing performed
- [ ] Retention policies followed
- [ ] Disposal procedures secure
- [ ] Transit protection enforced
- [ ] Storage security adequate

Application Security

- [ ] Secure development practices followed
- [ ] Security requirements defined
- [ ] Design reviews conducted
- [ ] Code reviews performed
- [ ] Security testing completed
- [ ] Vulnerability assessments done
- [ ] Web application firewalls deployed
- [ ] Input validation implemented
- [ ] Authentication mechanisms secure
- [ ] Session management proper
- [ ] Error handling appropriate

- [ ] Logging comprehensive

Endpoint Security

- [ ] Antivirus software deployed
- [ ] Signatures updated automatically
- [ ] Personal firewalls enabled
- [ ] Operating systems patched
- [ ] Applications updated regularly
- [ ] Unauthorized software prevented
- [ ] Removable media controlled
- [ ] Encryption enforced
- [ ] Screen locks configured
- [ ] Remote wipe capable
- [ ] Asset inventory current
- [ ] Configuration standards enforced

Security Operations

- [ ] SOC operational 24/7
- [ ] Monitoring tools configured properly
- [ ] Alerts tuned effectively
- [ ] Incident response procedures ready
- [ ] Forensic capabilities available
- [ ] Log collection comprehensive
- [ ] Log retention adequate
- [ ] Correlation rules effective
- [ ] Threat intelligence integrated
- [ ] Metrics tracked and reported
- [ ] Improvements implemented
- [ ] Team training current

Third-Party Security

- [ ] Vendor risk assessments performed
- [ ] Security requirements contractual
- [ ] Compliance verification done
- [ ] Access controlled strictly
- [ ] Monitoring active
- [ ] Incident notification required
- [ ] Data protection enforced
- [ ] Audit rights preserved
- [ ] Insurance requirements met
- [ ] Background checks completed
- [ ] NDAs executed
- [ ] Termination procedures defined

Incident Management

- ☐ Incident response plan documented
- ☐ Team members identified
- ☐ Contact information current
- ☐ Classification scheme defined
- ☐ Escalation procedures clear
- ☐ Communication plan ready
- ☐ Technical procedures detailed
- ☐ Evidence preservation understood
- ☐ Recovery procedures tested
- ☐ Lessons learned process active
- ☐ Training conducted regularly
- ☐ Exercises performed periodically

Compliance

- ☐ Regulatory requirements identified
- ☐ Standards adopted formally
- ☐ Framework implemented
- ☐ Controls mapped properly
- ☐ Testing performed regularly
- ☐ Evidence collected systematically
- ☐ Gaps identified and addressed
- ☐ Remediation tracked
- ☐ Audits scheduled
- ☐ Findings resolved timely
- ☐ Certifications maintained
- ☐ Improvements continuous

Security Awareness

- ☐ Training program established
- ☐ All employees trained
- ☐ Annual refresher required
- ☐ Role-based training provided
- ☐ Phishing simulations conducted
- ☐ Security tips communicated
- ☐ Incident reporting encouraged
- ☐ Policy acknowledgment required
- ☐ Metrics tracked
- ☐ Effectiveness measured
- ☐ Program updated regularly
- ☐ Management support visible