It Audit Checklist

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

IT Governance

- [ ] IT strategy aligned with business
- [ ] IT steering committee active
- [ ] Policies and procedures current
- [ ] Roles/responsibilities defined
- [ ] Decision rights clear
- [ ] Performance metrics established
- [ ] Risk management framework
- [ ] Compliance framework implemented
- [ ] Resource management effective
- [ ] Vendor management program
- [ ] Portfolio management active
- [ ] Benefits realization tracked

Infrastructure Security

- [ ] Network architecture documented
- [ ] Firewall rules appropriate
- [ ] Intrusion detection/prevention active
- [ ] Vulnerability scanning regular
- [ ] Patch management current
- [ ] Configuration management enforced
- [ ] Hardening standards applied
- [ ] Monitoring tools operational
- [ ] Logging comprehensive
- [ ] Incident response ready
- [ ] Forensic capability available
- [ ] Physical security adequate

Access Management

- [ ] Identity management system deployed
- [ ] Access provisioning controlled
- [ ] Privileged access managed
- [ ] Password policies enforced
- [ ] Multi-factor authentication enabled
- [ ] Single sign-on implemented
- [ ] Access reviews conducted
- [ ] Segregation of duties enforced

- [ ] Terminated access removed timely
- [ ] Service accounts managed
- [ ] Remote access secured
- [ ] Third-party access controlled

Data Management

- [ ] Data classification implemented
- [ ] Data inventory maintained
- [ ] Data flows mapped
- [ ] Encryption standards enforced
- [ ] Data retention policies followed
- [ ] Data disposal procedures secure
- [ ] Backup procedures tested
- [ ] Recovery capabilities verified
- [ ] Data integrity controls active
- [ ] Data quality monitored
- [ ] Master data managed
- [ ] Privacy controls implemented

Application Controls

- [ ] Input controls effective
- [ ] Processing controls adequate
- [ ] Output controls verified
- [ ] Interface controls tested
- [ ] Access controls enforced
- [ ] Change controls followed
- [ ] Error handling appropriate
- [ ] Audit trails comprehensive
- [ ] Business rules validated
- [ ] Calculations accurate
- [ ] Reports reliable
- [ ] Documentation complete

Change Management

- [ ] Change control board active
- [ ] Change requests documented
- [ ] Impact assessments performed
- [ ] Testing requirements defined
- [ ] Approval process followed
- [ ] Implementation planned
- [ ] Rollback procedures ready
- [ ] Documentation updated
- [ ] Communication effective
- [ ] Post-implementation review done
- [ ] Emergency changes controlled

- [ ] Success metrics tracked

Business Continuity

- [ ] BCP/DRP documented
- [ ] Business impact analysis current
- [ ] Recovery objectives defined
- [ ] Recovery strategies appropriate
- [ ] Plans tested regularly
- [ ] Test results documented
- [ ] Issues remediated
- [ ] Team members trained
- [ ] Contact lists current
- [ ] Alternate sites ready
- [ ] Backup systems functional
- [ ] Communication plans tested

Vendor Management

- [ ] Vendor inventory maintained
- [ ] Risk assessments performed
- [ ] Contracts reviewed
- [ ] SLAs monitored
- [ ] Performance measured
- [ ] Security requirements defined
- [ ] Compliance verified
- [ ] Issues tracked/resolved
- [ ] Relationships managed
- [ ] Financial stability monitored
- [ ] Exit strategies defined
- [ ] Knowledge transfer planned

Development Controls

- [ ] SDLC methodology followed
- [ ] Requirements documented
- [ ] Design reviews conducted
- [ ] Code reviews performed
- [ ] Testing comprehensive
- [ ] Security testing included
- [ ] User acceptance obtained
- [ ] Migration controlled
- [ ] Documentation complete
- [ ] Training provided
- [ ] Post-implementation reviewed
- [ ] Maintenance planned

IT Operations

- [ ] Operations procedures documented
- [ ] Job scheduling controlled
- [ ] Monitoring comprehensive
- [ ] Incident management effective
- [ ] Problem management mature
- [ ] Capacity planning performed
- [ ] Performance tuning done
- [ ] Batch processing controlled
- [ ] Output distribution secure
- [ ] Media handling secure
- [ ] Environmental controls adequate
- [ ] Maintenance scheduled

Compliance & Audit

- [ ] Regulatory requirements identified
- [ ] Compliance monitoring active
- [ ] Audit schedule maintained
- [ ] Findings tracked to closure
- [ ] Evidence retained properly
- [ ] Certifications current
- [ ] Training records complete
- [ ] Policy exceptions documented
- [ ] Violations addressed
- [ ] Continuous improvement shown
- [ ] External audits supported
- [ ] Management reporting done

Emerging Technology

- [ ] Cloud governance established
- [ ] Mobile device management active
- [ ] IoT security addressed
- [ ] AI/ML governance defined
- [ ] Blockchain controls considered
- [ ] RPA controls implemented
- [ ] API security managed
- [ ] Container security enforced
- [ ] DevOps security integrated
- [ ] Zero trust architecture planned
- [ ] Quantum readiness assessed
- [ ] Innovation managed