IT Audit Checklist

Phase 1: Planning

Organizational Structure Assessment

- ☐ Map organizational structure and departments
- ☐ Document how each department uses technology daily
- ☐ Identify team members' technology dependencies
- ☐ Understand network infrastructure importance by department
- ☐ Identify system components organization depends on most

Critical Network Operations Assessment

☐ Virtual and Physical Firewalls

- ☐ Firewall configuration review
- ☐ Rule effectiveness assessment
- ☐ Update status verification

☐ Computers and Network Devices

- ☐ Hardware inventory
- ☐ Device performance evaluation
- ☐ Age and replacement planning

☐ Network Performance and Speed

- ☐ Bandwidth utilization analysis
- ☐ Speed test results documentation

- ☐ Bottleneck identification

☐ Bring Your Own Device (BYOD) Policies

- ☐ Policy documentation review
- ☐ Employee compliance verification
- ☐ Security protocol assessment

☐ Wireless Access Points and Routers

- ☐ Coverage area mapping
- ☐ Security settings review
- ☐ Performance monitoring

☐ User Accounts and Access Controls

- ☐ User privilege review
- ☐ Account deactivation procedures
- ☐ Multi-factor authentication status

☐ Antivirus and Anti-Malware Software

- ☐ Software update verification
- ☐ Scan schedule confirmation
- ☐ Threat detection effectiveness

☐ Software Patch Management

- ☐ Patch deployment schedule
- ☐ Critical update identification
- ☐ System vulnerability assessment

☐ Automated Data Backups

- ☐ Backup schedule verification
- ☐ Recovery testing
- ☐ Storage location security

☐ Data Encryption Policies

- ☐ Encryption standard compliance
- ☐ Data at rest protection
- ☐ Data in transit security

☐ Cloud Storage Management

- ☐ Access control verification
- ☐ Data classification review
- ☐ Vendor security assessment

☐ Industry Compliance Requirements

- ☐ Regulatory requirement identification
- ☐ Compliance gap analysis
- ☐ Documentation review

Phase 2: Defining Goals 🎯

Primary Audit Objectives (Check all that apply)

- ☐ Mitigate security risks
- ☐ Test disaster recovery systems
- ☐ Minimize operating costs
- ☐ Improve system performance
- ☐ Ensure regulatory compliance
- ☐ Enhance user productivity

Control Measures Review

- ☐ Assess adequacy of current controls
- ☐ Evaluate control effectiveness
- ☐ Identify control gaps

☐ Document recommended improvements

System Performance Evaluation

☐ Server performance assessment

☐ Network performance review

☐ Individual device evaluation

☐ Response time analysis

Security Systems Review

☐ Current security posture assessment

☐ Threat landscape analysis

☐ Incident response capability

☐ Security awareness evaluation

Phase 3: Information Collection 📊

Interview Process

☐ Security Measures Interview

☐ Application users interviewed

☐ Security protocol understanding verified

☐ User experience documented

☐ Training needs identified

☐ System Usage Interview

- ☐ Daily workflow documentation
- ☐ Pain point identification
- ☐ Efficiency improvement suggestions
- ☐ Support requirement assessment

Questionnaire Distribution

☐ Security Awareness Questions

- ☐ Threat recognition capability
- ☐ Security protocol adherence
- ☐ Incident reporting procedures
- ☐ Password management practices

☐ Remote Work Assessment (if applicable)

- ☐ Home network security
- ☐ VPN usage compliance
- ☐ Device security measures
- ☐ Data handling procedures

☐ Network Understanding Evaluation

- ☐ Basic network operation knowledge
- ☐ Sensitive data protection awareness
- ☐ Communication security practices
- ☐ System malfunction recognition

Flowchart Creation

☐ Network Control Flowcharts

- ☐ Normal operation workflows
- ☐ Emergency response procedures
- ☐ Escalation paths documented
- ☐ Risk exposure points identified

☐ Team Distribution

- ☐ Flowcharts shared with relevant team members
- ☐ Understanding verification
- ☐ Feedback collection
- ☐ Updates implemented

Phase 4: Evaluation and Reporting 📈

Data Analysis

- ☐ Collected data compiled
- ☐ Industry-specific auditing software utilized
- ☐ Threat identification completed
- ☐ Weak point analysis finished

Report Generation

☐ Executive Summary

- ☐ Key findings highlighted
- ☐ Risk assessment summary
- ☐ Priority recommendations listed
- ☐ Cost-benefit analysis included

☐ Detailed Findings

- ☐ System vulnerabilities documented
- ☐ Performance issues identified
- ☐ Compliance gaps noted
- ☐ Security risks assessed

☐ Recommendations

- ☐ Immediate action items listed
- ☐ Long-term improvement plan
- ☐ Resource requirements identified
- ☐ Implementation timeline proposed

Action Plan Development

- ☐ Proactive threat addressing strategy
- ☐ Priority-based implementation schedule
- ☐ Resource allocation planning
- ☐ Success metrics definition

Post-Audit Actions ☑

Implementation Tracking

- ☐ Recommendation implementation status
- ☐ Progress milestone tracking
- ☐ Stakeholder communication
- ☐ Budget allocation monitoring

Ongoing Monitoring

- ☐ Regular security assessments scheduled
- ☐ Performance monitoring established
- ☐ Compliance verification routine

☐ Continuous improvement process

Documentation Updates

☐ Policies and procedures updated

☐ Training materials revised

☐ Emergency response plans updated

☐ Audit findings archived

Audit Completion Sign-off

Audit Conducted By: _____ **Date:** _____

Department/Team: _____ **Reviewed By:** _____

Next Audit Scheduled: _____ **Priority Level:** _____

Overall Risk Assessment:

☐ Low Risk ☐ Medium Risk ☐ High Risk

Immediate Actions Required:

☐ Yes (specify): _____

☐ No

This checklist is based on industry best practices for comprehensive IT auditing. Customize as needed for your organization's specific requirements and compliance needs.