ComDirect

IT Infrastructure Assessment Checklist

A Comprehensive Framework for Evaluating Your IT Environment and Identifying Optimization Opportunities

Servers & Compute • Networking • Storage & Backup • Security
End-User Computing • Cloud & SaaS • Documentation • Compliance

Technology Guide

ComDirect USA
comdirectusa.com

This checklist is a general-purpose assessment tool. Adapt the items to your organization's size, industry, and regulatory requirements. Not all items will apply to every environment.

How to Use This Guide

This checklist is designed to be used as a structured walk-through of your entire IT environment. It can serve as the basis for an internal self-assessment, a new-client onboarding review by a managed services provider, or a periodic health check to identify drift from best practices.

Assessment Process

1. Assign an owner for each section. The person closest to the technology should complete the assessment, but findings should be reviewed by a second set of eyes.

2. Work through each checklist item. Check the box if the item is fully satisfied. Leave it unchecked if it is not in place, partially implemented, or unknown.

3. Flag items marked with a risk indicator. These represent areas where gaps create immediate exposure to downtime, data loss, or security breach.

4. Score each section. Count checked items as a percentage of total items to produce a maturity score per domain.

5. Prioritize remediation. Address risk-flagged items first, then work through remaining gaps in order of business impact.

Scoring Guide

Above 90%: Well-managed environment with minor improvement opportunities.
70-89%: Functional but with notable gaps that should be addressed within 90 days.
50-69%: Significant risk exposure. Prioritize remediation immediately.
Below 50%: Critical gaps across multiple domains. Consider engaging a professional assessment.

Table of Contents

9. Assessment Summary and Scoring

Section 1

Servers and Compute Infrastructure

This section evaluates the health, configuration, and lifecycle status of your physical and virtual server infrastructure.

Hardware Inventory

- [ ] Complete inventory of all physical servers with make, model, serial number, and location
- [ ] Warranty and support contract status documented for every server
- [ ] End-of-life and end-of-support dates tracked; no servers running past vendor support
- [ ] Server room or data center environment monitored (temperature, humidity, power)
- [ ] Uninterruptible power supply (UPS) in place with load tested within the past 12 months
- [ ] Rack infrastructure labeled and cable management documented

Operating Systems

- [ ] All server operating systems are currently supported versions (no EOL OS in production)
- [ ] OS patching policy defined and enforced on a regular schedule (monthly or more frequent)
- [ ] Patch compliance reports generated and reviewed; non-compliant systems tracked
- [ ] Baseline hardening applied to all servers (CIS Benchmarks or equivalent)
- [ ] Unnecessary services and default accounts disabled on all servers

Virtualization

- [ ] Hypervisor platform and version documented; running a supported release
- [ ] VM sprawl assessed: all VMs have a documented owner and business purpose
- [ ] Resource utilization monitored; no hosts consistently above 80% CPU or memory
- [ ] High availability (HA) or failover clustering configured for critical workloads
- [ ] VM snapshots are temporary only; no long-running snapshots consuming storage

Risk Indicator

Any server running an end-of-life operating system or past its warranty expiration is a critical risk. These systems receive no security patches and have no vendor support for hardware failures.

Section 2

Network Infrastructure

This section evaluates your network topology, equipment, performance, and resilience.

Network Equipment

- [ ] Complete inventory of all routers, switches, firewalls, and wireless access points
- [ ] Firmware and software versions documented and current on all network devices
- [ ] No network equipment running past end-of-support or end-of-life
- [ ] Default credentials changed on all network devices; strong passwords enforced
- [ ] Management interfaces secured (SSH only, no telnet; management VLAN isolated)

Network Architecture

- [ ] Network topology diagram current and accurate (updated within past 6 months)
- [ ] VLANs implemented to segment traffic by function (servers, users, IoT, guest, voice)
- [ ] Inter-VLAN routing controlled by firewall rules, not wide-open access
- [ ] Guest network isolated from production with no path to internal resources
- [ ] DNS and DHCP services redundant; no single point of failure

WAN and Internet

- [ ] Internet circuit bandwidth matches current utilization with headroom for growth
- [ ] Redundant internet connectivity from diverse carriers or paths
- [ ] Automatic failover tested and verified between primary and backup circuits
- [ ] SD-WAN or traffic-shaping policies in place for application prioritization
- [ ] QoS configured and operational for voice and video traffic

Wireless

- [ ] Wireless access points provide full coverage in all occupied areas (no dead zones)
- [ ] Wi-Fi standards current (Wi-Fi 6 or later preferred for new deployments)
- [ ] WPA3 or WPA2-Enterprise authentication in use; no open or WPA/WEP networks
- [ ] Wireless intrusion detection enabled to identify rogue access points
- [ ] BYOD and IoT devices on separate SSIDs and VLANs from corporate endpoints

Risk Indicator

A flat network with no VLAN segmentation means a single compromised device can reach every system in the environment. This is the most common enabler of lateral movement in cyberattacks.

Section 3

Storage and Backup

This section evaluates data storage, backup coverage, and recovery readiness.

Storage Infrastructure

- [ ] Complete inventory of all storage systems (SAN, NAS, DAS) with capacity and utilization
- [ ] Storage capacity planning in place; no volumes above 85% utilization without a growth plan
- [ ] RAID configurations appropriate for workload (no single-disk or degraded arrays)
- [ ] Storage performance monitored; latency and IOPS within acceptable thresholds
- [ ] Data deduplication and compression enabled where supported

Backup Configuration

- [ ] All critical data is backed up, including: file servers, databases, email, application data, and system state
- [ ] Backup schedule defined and documented (daily incremental, weekly full, or equivalent)
- [ ] At least one backup copy stored offsite or in the cloud (3-2-1 rule)
- [ ] Backup encryption enabled for all offsite and cloud copies
- [ ] Backup retention periods defined and aligned with business and regulatory requirements
- [ ] Backup jobs monitored daily; failures investigated and resolved within 24 hours

Recovery Readiness

- [ ] Recovery Point Objective (RPO) and Recovery Time Objective (RTO) defined for each critical system
- [ ] Test restores performed at least quarterly for critical systems
- [ ] Full disaster recovery test (bare-metal restore or site failover) performed annually
- [ ] Recovery documentation exists and is accessible to the recovery team (not only on the failed system)
- [ ] Cloud-based or secondary-site recovery capability in place for business continuity

Risk Indicator

Backups that have never been test-restored are not backups. They are assumptions. A backup system that runs without errors does not guarantee that the data can be restored in a real disaster. Test restores are non-negotiable.

Section 4

Security Controls

This section evaluates the security posture across identity, endpoint, network, and organizational controls.

Identity and Access

- [ ] Multi-factor authentication (MFA) enforced for all users, not just administrators
- [ ] Single sign-on (SSO) implemented for all supported applications
- [ ] Privileged accounts inventoried and managed through a PAM solution or equivalent controls
- [ ] Access reviews conducted at least quarterly for privileged access, semi-annually for all access
- [ ] Offboarding process disables all accounts within 24 hours of termination; verified by audit log
- [ ] Password policy enforces minimum 14 characters or passphrase; no forced rotation without MFA

Endpoint Security

- [ ] Endpoint Detection and Response (EDR) deployed on all endpoints (workstations and servers)
- [ ] EDR managed and monitored 24/7 with alerting and response procedures defined
- [ ] Full-disk encryption enabled on all laptops and portable devices (BitLocker, FileVault)
- [ ] USB and removable media policy enforced through endpoint management
- [ ] Mobile Device Management (MDM) deployed for all company-owned mobile devices

Network Security

- [ ] Firewall rules reviewed and cleaned up within the past 12 months; no "any-any" rules
- [ ] Intrusion detection/prevention system (IDS/IPS) in place and actively monitored
- [ ] DNS filtering or web proxy blocks access to known malicious domains
- [ ] Email security: advanced anti-phishing, attachment sandboxing, and DMARC/DKIM/SPF configured
- [ ] Vulnerability scanning performed at least monthly; critical findings remediated within 30 days

Security Operations

- [ ] Security awareness training conducted for all employees at least annually
- [ ] Phishing simulation tests conducted at least quarterly with results tracked
- [ ] Incident response plan documented, tested via tabletop exercise within the past 12 months
- [ ] Cyber insurance policy in place with coverage appropriate for organization size and risk
- [ ] Penetration test conducted within the past 12 months by a qualified third party

Risk Indicator

No MFA on email and VPN accounts is the single most exploitable gap in most organizations. Compromised

credentials with no second factor are responsible for the majority of successful breaches.

Risk Indicator

No MFA on email and VPN accounts is the single most exploitable gap in most organizations. Compromised

credentials with no second factor are responsible for the majority of successful breaches.

Section 5

End-User Computing

This section evaluates the devices, software, and support experience for all end users in the organization.

Hardware Standards

- [ ] All workstations and laptops meet a defined minimum hardware specification
- [ ] Device lifecycle policy defined (typically 4-year replacement cycle for laptops)
- [ ] No devices in production past their planned lifecycle without documented exception
- [ ] Standardized hardware models to reduce support complexity and parts inventory
- [ ] Asset tracking system in place with assignment records for all devices

Software Management

- [ ] Operating systems current and receiving security updates (no Windows 10 past EOL, etc.)
- [ ] Application patching automated for common software (browsers, PDF readers, Java, etc.)
- [ ] Software inventory maintained; all installed applications are licensed and approved
- [ ] Application deployment standardized through endpoint management (Intune, SCCM, etc.)
- [ ] Shadow IT monitored: unauthorized SaaS sign-ups detected through CASB or log analysis

Printing and Peripherals

- [ ] Print infrastructure consolidated and managed (no unmanaged consumer printers on the network)
- [ ] Secure print (badge release or PIN) in place for environments with sensitive documents
- [ ] Printer firmware updated and default admin credentials changed
- [ ] Conference room AV equipment standardized and functioning reliably

User Support

- [ ] Help desk SLAs defined: response time, resolution time, and escalation procedures
- [ ] Ticket system in use for all support requests (no hallway or ad-hoc support only)
- [ ] User satisfaction measured through periodic survey or ticket-close feedback
- [ ] New employee onboarding: device provisioned, accounts created, and access ready before start date
- [ ] Self-service options available for common tasks (password reset, software request)

Risk Indicator

Devices running end-of-life operating systems (such as Windows 10 after October 2025) no longer receive security patches. Every day past EOL increases exposure to unpatched vulnerabilities.

Section 6

Cloud and SaaS Management

This section evaluates your management and governance of cloud infrastructure and SaaS applications.

Cloud Infrastructure (IaaS/PaaS)

- [ ] All cloud accounts (AWS, Azure, GCP) inventoried with designated owners
- [ ] Root/global admin accounts secured with MFA and restricted to break-glass use only
- [ ] Cloud resource tagging policy enforced for cost allocation and ownership tracking
- [ ] Monthly cost reviews conducted; unexpected spend increases investigated
- [ ] Cloud security posture management (CSPM) tool in place to detect misconfigurations
- [ ] Cloud backup and snapshot policies defined and tested for all production workloads

SaaS Application Governance

- [ ] Inventory of all SaaS applications in use, including department-owned subscriptions
- [ ] SSO integration implemented for all SaaS applications that support it
- [ ] Data residency requirements met for all SaaS applications handling regulated data
- [ ] SaaS vendor security reviewed: SOC 2 reports, BAAs, DPAs collected and current
- [ ] Offboarding process includes revocation of access to all SaaS applications

Microsoft 365 / Google Workspace

- [ ] MFA enforced for all users without exception
- [ ] Conditional access policies configured (block legacy auth, require managed devices, etc.)
- [ ] Email forwarding rules audited; no unauthorized auto-forwarding to external addresses
- [ ] Data Loss Prevention (DLP) policies configured for sensitive data in email and file sharing
- [ ] Audit logging enabled and retained for at least 90 days
- [ ] Third-party backup in place (native retention is not a substitute for backup)

Shadow IT Reality

The average mid-market organization uses 3-4x more SaaS applications than IT is aware of. Departments sign up for tools with corporate credit cards, creating unmanaged data stores and ungoverned access. A SaaS discovery and governance process is essential.

Section 7

Documentation and Knowledge Management

Documentation is not overhead. It is operational infrastructure. Without it, your organization is one resignation or sick day away from losing critical institutional knowledge.

Network and Systems Documentation

- [ ] Network topology diagram: current, accurate, and accessible to the team
- [ ] IP address management (IPAM): all subnets, VLANs, and static assignments documented
- [ ] Server build documentation: OS, applications, configurations, dependencies for each server
- [ ] Firewall rule documentation: purpose and business justification for each rule
- [ ] DNS records documented with ownership and purpose for each zone and record

Operational Runbooks

- [ ] Standard operating procedures (SOPs) for recurring tasks: patching, backups, user provisioning
- [ ] Escalation procedures documented: who to call, when, and in what order
- [ ] Vendor contact list: account numbers, support phone numbers, and contract details
- [ ] Disaster recovery runbook: step-by-step procedures for restoring each critical system
- [ ] After-hours and on-call procedures documented and current

Credential Management

- [ ] All shared/service account credentials stored in an enterprise password manager
- [ ] No credentials stored in spreadsheets, sticky notes, browser password stores, or plain text files
- [ ] Service account credentials rotated on a defined schedule
- [ ] Break-glass (emergency access) credentials documented, secured, and tested

Change Management

- [ ] All changes to production systems follow a documented change management process
- [ ] Changes are logged with description, approver, implementer, and rollback plan
- [ ] Emergency change process defined for urgent issues that cannot wait for standard approval
- [ ] Post-change verification performed and documented for every change

Risk Indicator

If your IT environment cannot be fully operated by someone who was not part of building it, your documentation is insufficient. The "bus factor" (what happens if a key person is unavailable) is a real operational risk, not a theoretical exercise.

Section 8

Compliance and Governance

This section evaluates organizational readiness for regulatory compliance and IT governance. Adapt the items below to your specific regulatory requirements.

Regulatory Awareness

- [ ] All applicable regulations identified (HIPAA, SOX, PCI-DSS, state privacy laws, etc.)
- [ ] Compliance responsibilities assigned to specific individuals or roles
- [ ] Regulatory changes monitored and assessed for impact on IT controls
- [ ] Legal and compliance teams engaged in IT policy development and review

Policy Framework

- [ ] Information Security Policy: board-approved, reviewed annually, communicated to all staff
- [ ] Acceptable Use Policy: defines permitted use of company technology and data
- [ ] Data Classification Policy: defines sensitivity levels and handling requirements
- [ ] Incident Response Policy: defines breach notification requirements and timelines
- [ ] Data Retention and Disposal Policy: defines retention periods and destruction procedures
- [ ] Remote Work / BYOD Policy: defines security requirements for remote access and personal devices

Audit Readiness

- [ ] Evidence library maintained with current documentation for all required controls
- [ ] Access review documentation retained for at least the current audit period
- [ ] Change management records retained and retrievable for audit
- [ ] Risk assessment performed within the past 12 months and documented
- [ ] Third-party vendor compliance documentation current (SOC 2 reports, BAAs, DPAs)
- [ ] Internal audit or readiness review conducted prior to external audit engagement

Business Continuity

- [ ] Business Impact Analysis (BIA) completed identifying critical systems and processes
- [ ] Business continuity plan documented and communicated to key stakeholders
- [ ] Recovery priorities (RPO/RTO) defined for all critical systems based on BIA
- [ ] Annual business continuity exercise conducted with results documented

Governance Foundation

Compliance is the floor, not the ceiling. A mature IT governance program goes beyond checking regulatory boxes to align technology decisions with business strategy, manage risk proactively, and demonstrate due diligence to

customers, partners, and insurers.

Governance Foundation

Compliance is the floor, not the ceiling. A mature IT governance program goes beyond checking regulatory boxes to align technology decisions with business strategy, manage risk proactively, and demonstrate due diligence to

customers, partners, and insurers.

Section 9

Assessment Summary and Scoring

Use the table below to record your score for each section. Count the number of checked items as a percentage of total checklist items in that section.

Section	Items	Checked	Score (%)
1. Servers and Compute	16		
2. Network Infrastructure	19		
3. Storage and Backup	16		
4. Security Controls	20		
5. End-User Computing	18		
6. Cloud and SaaS Management	17		
7. Documentation & Knowledge Mgmt	17		
8. Compliance and Governance	16		
TOTAL	**139**		

Interpreting Your Score

90-100%: Strong IT posture. Focus on continuous improvement and emerging threats. Reassess annually.

70-89%: Functional environment with notable gaps. Build a 90-day remediation plan targeting the highest-risk unchecked items first.

50-69%: Significant exposure across multiple domains. Immediate action required on risk-flagged items. Consider engaging a professional assessment to prioritize remediation.

Below 50%: Critical gaps that put the organization at material risk of downtime, data loss, or breach. Executive attention and dedicated resources are needed.

What to Do Next

1. Address all risk-flagged items immediately. These represent the highest-probability, highest-impact exposures.

2. Build a prioritized remediation plan organized by business impact, not by section order.

3. Assign owners and deadlines to each remediation item.

4. Reassess in 90 days to measure progress.

5. Repeat this assessment annually or after any major infrastructure change.

About ComDirect USA

ComDirect USA is a full-service technology partner specializing in enterprise infrastructure, cybersecurity, cloud architecture, and managed IT services. With offices in Irvine, California, and Meridian, Idaho, we serve organizations across healthcare, legal, financial services, manufacturing, and logistics.

Need help with your assessment? Contact us.

Phone: 949.208.8800 | Toll Free: 800.733.7030

Email: info@comdirectusa.com | Web: comdirectusa.com