ComDirect

Cybersecurity Readiness Assessment

A Self-Assessment Guide to Evaluate Your Organization's Security Posture

Technology Guide

ComDirect USA
comdirectusa.com

How to Use This Assessment

This guide is designed as a structured self-assessment that any organization can use to evaluate its cybersecurity readiness. Each section covers a critical security domain with checklist items scored on a maturity scale.

Scoring Each Item

For each checklist item, assign a score from 0 to 3:

- 0 = Not implemented. No capability exists in this area.
- 1 = Partially implemented. Some controls exist but are incomplete, inconsistent, or not enforced.
- 2 = Fully implemented. Controls are in place and operating, but not regularly tested or reviewed.
- 3 = Mature. Controls are implemented, regularly tested, continuously monitored, and improved based on findings.

Items marked with a red risk indicator represent critical controls whose absence creates immediate, exploitable exposure. These should be prioritized regardless of overall score.

Scoring Guide

Above 80%: Strong security posture. Focus on continuous improvement and advanced capabilities.
60-79%: Functional baseline with notable gaps. Build a 90-day remediation plan.
40-59%: Significant exposure. Immediate action required on critical items.
Below 40%: Material risk across multiple domains. Executive attention and professional assessment recommended.

Table of Contents

11. **Assessment Summary and Scoring**
12. **Building Your Remediation Roadmap**

Section 1

Identity and Access Management

Identity is the primary attack surface for most organizations. Compromised credentials are the leading cause of data breaches, and weak access controls enable attackers to escalate privileges and move laterally once inside.

Authentication Controls

- [ ] Multi-factor authentication (MFA) enforced for all users on all externally accessible systems (email, VPN, cloud apps, RDP)
- [ ] MFA method is phishing-resistant (FIDO2 hardware keys, platform authenticators) rather than SMS-based OTP
- [ ] Legacy authentication protocols (NTLM, basic auth, POP/IMAP without OAuth) disabled or blocked
- [ ] Conditional access policies enforce device compliance, location, and risk level before granting access
- [ ] Self-service password reset requires identity verification and is logged for audit

Access Governance

- [ ] Role-based access control (RBAC) implemented with documented role definitions and permission mappings
- [ ] Least-privilege principle enforced: users have access only to systems required for their job function
- [ ] Access reviews conducted quarterly for privileged accounts, semi-annually for all accounts
- [ ] Offboarding process disables all accounts and revokes all access within 24 hours of termination
- [ ] Joiner/mover/leaver automation in place: access provisioned and adjusted based on HR system events

Privileged Access

- [ ] All administrative accounts inventoried with documented owners and business justification
- [ ] Privileged credentials stored in a password vault with automatic rotation
- [ ] Just-in-time (JIT) access implemented: admin rights granted temporarily with approval, not permanently assigned
- [ ] Privileged sessions recorded and available for forensic review
- [ ] Separate admin accounts used for privileged work (no daily-use accounts with admin rights)

Critical Risk

MFA on email and VPN is non-negotiable. Compromised credentials without a second factor are the entry point for the vast majority of successful attacks, including business email compromise, ransomware, and data theft.

Section 2

Endpoint Protection

Every workstation, laptop, server, and mobile device is a potential entry point. Endpoint protection must cover detection, prevention, and response across all device types in your environment.

Endpoint Detection and Response (EDR)

- ☐ EDR solution deployed on all endpoints: workstations, laptops, and servers (Windows, macOS, Linux)
- ☐ EDR is managed and monitored 24/7 by qualified analysts (internal SOC or managed detection and response provider)
- ☐ EDR policies configured to block known malware, detect behavioral anomalies, and isolate compromised endpoints
- ☐ EDR alert investigation and response SLAs defined (e.g., critical alerts triaged within 15 minutes)
- ☐ EDR agent health monitored: alerts generated when agents go offline, are disabled, or are not reporting

Device Hardening

- ☐ Operating system hardening baselines applied to all endpoints (CIS Benchmarks or equivalent)
- ☐ Full-disk encryption enabled on all laptops and portable devices (BitLocker, FileVault, LUKS)
- ☐ Local administrator rights removed from standard user accounts
- ☐ USB and removable media access controlled by policy (blocked, read-only, or logged)
- ☐ Automatic screen lock enforced after inactivity (maximum 5 minutes for unattended devices)
- ☐ BIOS/UEFI password set and Secure Boot enabled on all managed devices

Mobile Device Management

- ☐ MDM/UEM solution deployed for all company-owned mobile devices
- ☐ BYOD devices accessing corporate data enrolled in MDM with containerized workspaces
- ☐ Remote wipe capability verified and tested for lost or stolen devices
- ☐ Mobile device compliance policies enforced (PIN/biometric lock, OS version, no jailbreak/root)
- ☐ Corporate app distribution managed through enterprise app store (no sideloading)

Critical Risk

Endpoints without EDR are blind spots. Traditional antivirus catches known signatures but misses fileless attacks, living-off-the-land techniques, and zero-day exploits. If you do nothing else, deploy managed EDR on every endpoint.

Section 3

Network Security

Network security controls protect the pathways between users, applications, and data. Even with strong identity and endpoint controls, network-layer weaknesses enable reconnaissance, lateral movement, and data exfiltration.

Firewall and Perimeter

- [ ] Next-generation firewall (NGFW) deployed at all internet egress points with application-layer inspection
- [ ] Firewall rules reviewed and cleaned within the past 12 months; no overly permissive "any-any" rules remain
- [ ] Inbound access limited to explicitly required services; all other inbound traffic denied by default
- [ ] Firewall firmware current and within vendor support lifecycle
- [ ] Firewall change management process documented and followed for every rule modification

Network Segmentation

- [ ] Network segmented into zones by function (servers, users, IoT, guest, voice, management)
- [ ] Inter-zone traffic controlled by firewall rules based on least-privilege (not wide-open VLAN routing)
- [ ] Guest and IoT networks fully isolated from production with no path to sensitive resources
- [ ] Server-to-server (east-west) traffic monitored for anomalous lateral movement
- [ ] Critical systems (financial, healthcare, PII stores) in dedicated segments with enhanced monitoring

DNS and Web Security

- [ ] DNS filtering in place to block access to known malicious, phishing, and command-and-control domains
- [ ] HTTPS inspection enabled for encrypted web traffic (with appropriate privacy exceptions)
- [ ] Web application firewall (WAF) deployed in front of any internet-facing web applications
- [ ] DNSSEC enabled for all externally published DNS zones

Wireless Security

- [ ] WPA3 or WPA2-Enterprise authentication required for all corporate wireless networks
- [ ] Wireless intrusion detection enabled to identify rogue access points
- [ ] Wireless network access segmented (corporate devices on one SSID/VLAN, BYOD/guests on another)

Critical Risk

A flat, unsegmented network means one compromised device can reach every system in the environment. Network segmentation is the single most effective control for limiting the blast radius of an attack.

Critical Risk

A flat, unsegmented network means one compromised device can reach every system in the environment. Network segmentation is the single most effective control for limiting the blast radius of an attack.

Section 4

Email and Communication Security

Email remains the number one attack vector. Phishing, business email compromise (BEC), and malicious attachments account for the majority of initial access in successful cyberattacks.

Email Gateway Protection

- [ ] Advanced email security deployed with AI/ML-based phishing detection beyond basic spam filtering
- [ ] Attachment sandboxing: suspicious attachments detonated in an isolated environment before delivery
- [ ] URL rewriting and time-of-click analysis: links in emails checked at the moment the user clicks, not just at delivery
- [ ] Impersonation protection: policies detect and flag emails that spoof executive names or internal domains
- [ ] External email tagging: messages from outside the organization are visually flagged with a banner or tag

Email Authentication

- [ ] SPF (Sender Policy Framework) records published and enforced for all sending domains
- [ ] DKIM (DomainKeys Identified Mail) signing enabled for all outbound email
- [ ] DMARC policy set to "reject" or "quarantine" (not just "none") with aggregate reporting enabled
- [ ] DMARC reports monitored to identify unauthorized senders and spoofing attempts

Business Email Compromise Prevention

- [ ] Mail flow rules block auto-forwarding to external addresses (or require approval)
- [ ] High-value actions (wire transfers, vendor payment changes, HR data requests) require out-of-band verification, not just email approval
- [ ] Mailbox audit logging enabled and retained for at least 90 days
- [ ] Delegated mailbox access reviewed quarterly for appropriateness

Collaboration Platform Security

- [ ] Teams/Slack/Zoom: external sharing policies defined and enforced
- [ ] File sharing links default to internal-only; external sharing requires explicit action and expiration
- [ ] Guest access to collaboration platforms reviewed quarterly and expired when no longer needed

BEC Is Not Just Phishing

Business Email Compromise is a targeted, financially motivated attack where attackers impersonate executives or vendors to redirect payments or steal sensitive data. Unlike mass phishing, BEC emails contain no malware and no

malicious links, making them invisible to traditional email security. Process controls (verification procedures for financial transactions) are the primary defense.

BEC Is Not Just Phishing

Business Email Compromise is a targeted, financially motivated attack where attackers impersonate executives or vendors to redirect payments or steal sensitive data. Unlike mass phishing, BEC emails contain no malware and no

malicious links, making them invisible to traditional email security. Process controls (verification procedures for financial transactions) are the primary defense.

Section 5

Data Protection

Data is the ultimate target of most attacks. Protecting data requires understanding where it lives, how it moves, who can access it, and what happens when controls fail.

Data Classification and Inventory

- ☐ Data classification policy defined with clear categories (Public, Internal, Confidential, Restricted)
- ☐ Sensitive data locations identified and documented (databases, file shares, cloud storage, email, endpoints)
- ☐ Data flow mapping completed: how does sensitive data move between systems, users, and third parties?
- ☐ Shadow data stores identified: data in unapproved locations (personal cloud storage, USB drives, local copies)

Encryption

- ☐ Data at rest encrypted with AES-256 or equivalent on all servers, databases, and storage containing sensitive data
- ☐ Data in transit protected by TLS 1.2 or higher; TLS 1.0 and 1.1 disabled across all services
- ☐ Email encryption available for sensitive communications (transport-layer TLS and message-level encryption)
- ☐ Encryption key management centralized with keys stored separately from encrypted data
- ☐ Full-disk encryption on all portable devices verified through endpoint management reporting

Data Loss Prevention (DLP)

- ☐ DLP policies configured to detect and block sensitive data leaving the organization via email, web upload, and removable media
- ☐ DLP rules tuned to minimize false positives while catching genuine exfiltration attempts
- ☐ Cloud DLP policies applied to SaaS file sharing (OneDrive, SharePoint, Google Drive, Dropbox)
- ☐ DLP incidents reviewed and investigated; repeated violations escalated to management

Backup and Recovery

- ☐ All critical data backed up following the 3-2-1-1 rule (3 copies, 2 media, 1 offsite, 1 immutable)
- ☐ Backups tested with verified restore at least quarterly for critical systems
- ☐ Backup infrastructure protected from ransomware: immutable storage, separate credentials, isolated network
- ☐ Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) defined and validated

through testing

Critical Risk

Backups without immutable or air-gapped copies are vulnerable to ransomware that specifically targets backup infrastructure. If ransomware can encrypt or delete your backups, your recovery options are limited to paying the ransom or rebuilding from scratch.

Section 6

Vulnerability and Patch Management

Unpatched systems are open invitations. Known vulnerabilities with available patches are the most commonly exploited attack vector after credential compromise. A disciplined patching program closes these doors before attackers walk through them.

Vulnerability Scanning

- [ ] Automated vulnerability scanning runs at least monthly across all internal and external-facing systems
- [ ] Scan results reviewed and triaged within 5 business days of each scan
- [ ] Critical and high-severity vulnerabilities remediated within 30 days of discovery
- [ ] Medium-severity vulnerabilities remediated within 90 days of discovery
- [ ] External penetration test conducted annually by a qualified third party
- [ ] Web application security testing (DAST/SAST) performed for all internet-facing applications

Patch Management

- [ ] OS patching policy defined and enforced: critical patches within 14 days, routine patches within 30 days
- [ ] Third-party application patching automated for common software (browsers, PDF readers, Java, productivity suites)
- [ ] Patch compliance reports generated monthly with non-compliant systems tracked and escalated
- [ ] Emergency patching process defined for actively exploited zero-day vulnerabilities (target: 72 hours)
- [ ] Patch testing performed in a non-production environment before deployment to critical systems
- [ ] Server patching coordinated with maintenance windows and includes rollback procedures

Asset Discovery

- [ ] Continuous asset discovery running to identify new devices and services on the network
- [ ] Shadow IT devices detected and either onboarded into management or removed from the network
- [ ] All discovered assets mapped to an owner and included in the vulnerability scanning scope

The Patching Window

The average time from vulnerability disclosure to active exploitation has shrunk from 45 days to under 15 days for critical vulnerabilities. If your patching cycle is monthly, you are leaving a window of exposure. For internet-facing systems, patch critical vulnerabilities within days, not weeks.

Section 7

Incident Response Readiness

Every organization will experience a security incident. The difference between a minor disruption and a catastrophic breach often comes down to how prepared you are to detect, contain, and recover from it.

Incident Response Plan

- ☐ Written incident response plan exists and has been reviewed within the past 12 months
- ☐ Plan defines incident classification criteria (severity levels) and response procedures for each level
- ☐ Roles and responsibilities assigned: incident commander, technical lead, communications lead, legal liaison
- ☐ Contact information for all response team members includes personal cell phones (not just office numbers)
- ☐ Plan includes after-hours and weekend activation procedures
- ☐ Plan is accessible from multiple locations (not only stored on systems that may be compromised)

Detection and Analysis

- ☐ SIEM or log aggregation platform in place, collecting logs from endpoints, network devices, identity providers, and cloud platforms
- ☐ Alert correlation rules configured to detect multi-stage attacks across log sources
- ☐ Alert triage and investigation performed within defined SLAs (critical: 15 min, high: 1 hour)
- ☐ Threat intelligence feeds integrated to enrich alerts with context on known threat actors and TTPs
- ☐ Indicators of compromise (IOCs) can be searched across historical logs for retrospective threat hunting

Containment and Recovery

- ☐ Endpoint isolation capability: ability to disconnect a compromised device from the network remotely within minutes
- ☐ Account suspension automation: ability to disable compromised accounts and revoke active sessions immediately
- ☐ Forensic imaging capability: ability to capture a forensic disk image before remediation destroys evidence
- ☐ Predefined containment playbooks for common scenarios (ransomware, BEC, data exfiltration, insider threat)
- ☐ Relationship established with an external incident response firm for surge capacity during major incidents

Post-Incident Activities

- ☐ Post-incident review (blameless retrospective) conducted within 14 days of every significant incident
- ☐ Lessons learned documented and tracked through to control improvements
- ☐ Breach notification procedures and timelines documented per applicable regulations
- ☐ Cyber insurance carrier notification procedures documented and tested

Critical Risk

An incident response plan that has never been tested through a tabletop exercise is a document, not a capability. Under the stress of an active incident, untested plans fail at the points where assumptions meet reality. Test at least twice per year.

Section 8

Security Awareness and Training

Technology controls cannot prevent every attack. Users remain the last line of defense against phishing, social engineering, and insider threats. A well-trained workforce is a security control in its own right.

Security Awareness Program

- ☐ Formal security awareness training program exists and is mandatory for all employees
- ☐ Training completed by all employees at least annually, with new hires trained within 30 days of start date
- ☐ Training content updated at least annually to reflect current threats and attack techniques
- ☐ Training covers: phishing recognition, password hygiene, physical security, data handling, social engineering, and incident reporting
- ☐ Completion tracked and reported to management; non-completion escalated

Phishing Simulation

- ☐ Simulated phishing campaigns conducted at least quarterly
- ☐ Campaigns use realistic scenarios that reflect actual threats targeting your industry
- ☐ Click rates tracked over time to measure improvement (industry benchmark: < 5% click rate)
- ☐ Employees who click receive immediate just-in-time training explaining the indicators they missed
- ☐ Repeat offenders receive additional targeted training and, if necessary, management involvement

Security Culture

- ☐ Employees know how to report suspicious emails, calls, or activity (clear, well-publicized reporting channel)
- ☐ Reporting is encouraged without blame: employees feel safe reporting mistakes and near-misses
- ☐ Security team provides regular communications (newsletter, intranet posts, Slack channel) with threat updates and tips
- ☐ Executive leadership visibly participates in security training and communicates its importance
- ☐ Security awareness metrics reported to executive leadership at least quarterly

Beyond Compliance Training

Annual compliance-driven training (click through slides, pass a quiz) satisfies a regulatory checkbox but does not change behavior. Effective programs combine short-form monthly micro-training, realistic phishing simulations, positive reinforcement for good security behavior, and visible executive sponsorship.

Section 9

Cloud and SaaS Security

Cloud infrastructure and SaaS applications now host the majority of business data and processes. Misconfigured cloud environments are among the fastest-growing sources of data breaches.

Cloud Infrastructure Security

- [ ] Cloud Security Posture Management (CSPM) tool deployed to continuously scan for misconfigurations
- [ ] Root/global admin accounts protected with MFA and restricted to break-glass use with monitored access
- [ ] Cloud IAM policies follow least-privilege: no wildcard permissions, no overly broad roles
- [ ] Cloud resource logging enabled (CloudTrail, Azure Activity Log, GCP Audit Logs) and sent to SIEM
- [ ] Public access to storage buckets and databases blocked by default; exceptions require documented approval
- [ ] Infrastructure-as-code templates validated against security policies before deployment

SaaS Security

- [ ] Complete SaaS application inventory maintained, including department-owned subscriptions
- [ ] SSO integration implemented for all SaaS applications that support it
- [ ] OAuth application consent reviewed: third-party apps with access to corporate data audited and unauthorized apps revoked
- [ ] SaaS data sharing settings reviewed: external sharing restricted to approved domains or disabled
- [ ] SaaS vendor SOC 2 reports collected and reviewed annually

Microsoft 365 / Google Workspace Specific

- [ ] Conditional access policies block legacy authentication protocols
- [ ] Mailbox audit logging enabled with retention of at least 90 days
- [ ] Email forwarding rules audited: no unauthorized auto-forwarding to external addresses
- [ ] SharePoint/OneDrive/Google Drive external sharing policies defined and enforced
- [ ] Third-party app registrations reviewed and restricted to approved publishers
- [ ] Admin activity alerts configured for high-risk actions (role assignment, policy changes, mailbox delegation)

Critical Risk

Publicly accessible cloud storage (S3 buckets, Azure Blob containers, GCS buckets) is one of the most common causes of large-scale data exposure. A single misconfigured bucket can expose millions of records. CSPM tools catch

these misconfigurations before attackers do.

Critical Risk

Publicly accessible cloud storage (S3 buckets, Azure Blob containers, GCS buckets) is one of the most common causes of large-scale data exposure. A single misconfigured bucket can expose millions of records. CSPM tools catch

these misconfigurations before attackers do.

Section 10

Compliance Gap Analysis

This section helps you identify gaps between your current security controls and the requirements of common regulatory frameworks. Check each item if you can demonstrate compliance with evidence.

HIPAA (Healthcare)

- [ ] Risk assessment completed within the past 12 months identifying all systems that handle ePHI
- [ ] Business Associate Agreements (BAAs) in place with all vendors that handle ePHI
- [ ] ePHI encrypted at rest and in transit on all systems
- [ ] Audit logs capture all access to ePHI with retention per policy
- [ ] Workforce training on HIPAA privacy and security completed annually
- [ ] Breach notification procedures documented with 60-day notification timeline

PCI-DSS (Payment Card Industry)

- [ ] Cardholder data environment (CDE) identified and segmented from the general network
- [ ] Cardholder data encrypted at rest and in transit; tokenization used where possible
- [ ] MFA required for all access to the CDE
- [ ] Quarterly internal and external vulnerability scans completed (ASV for external)
- [ ] Annual penetration test of the CDE completed
- [ ] Log monitoring and anomaly detection in place for all CDE systems

SOC 2 (Service Organizations)

- [ ] Information security policy reviewed and approved annually by management
- [ ] Access controls documented and enforced with periodic access reviews
- [ ] Change management process formalized with documented approvals and testing
- [ ] Incident response plan documented and tested via tabletop exercise
- [ ] Vendor risk management program in place with annual reviews
- [ ] System monitoring and alerting in place with defined response procedures

State Privacy Laws (CCPA, CPRA, etc.)

- [ ] Data inventory identifies all personal information collected, stored, and shared
- [ ] Privacy policy published and accessible, reflecting current data practices
- [ ] Consumer rights request process operational (access, deletion, opt-out)
- [ ] Data processing agreements in place with all third parties receiving personal information
- [ ]

Data retention and disposal practices aligned with stated privacy policy

Gap Analysis Is Not Compliance

This section identifies where your controls fall short of regulatory requirements. Closing the gaps requires remediation planning, implementation, evidence collection, and in many cases, independent audit or certification. Use this analysis as a starting point, then engage qualified compliance professionals for formal validation.

Section 11

Assessment Summary and Scoring

Record your score for each section below. For each checklist item, score 0-3 (Not implemented / Partial / Implemented / Mature). Calculate the percentage of maximum possible points.

Section	Max Points	Your Score	Percentage
1. Identity & Access Management	45		
2. Endpoint Protection	48		
3. Network Security	42		
4. Email & Communication Security	45		
5. Data Protection	48		
6. Vulnerability & Patch Mgmt	45		
7. Incident Response Readiness	48		
8. Security Awareness & Training	42		
9. Cloud & SaaS Security	51		
10. Compliance Gap Analysis	69		
TOTAL	**483**		

Interpreting Your Score

Above 80% (387+ points): Strong cybersecurity posture. You have mature controls across most domains. Focus on advanced capabilities, threat hunting, and continuous improvement.

60-79% (290-386 points): Solid foundation with gaps that need attention. Build a 90-day remediation plan targeting critical-risk items first, then systematic improvement across weaker sections.

40-59% (193-289 points): Significant exposure in multiple areas. Prioritize critical-risk items immediately. Consider engaging a professional security assessment to validate findings and guide remediation.

Below 40% (< 193 points): Material risk that requires urgent executive attention. Engage a qualified cybersecurity firm for a formal assessment and remediation roadmap.

Section 12

Building Your Remediation Roadmap

A long list of findings without a plan is overwhelming. Structure your remediation as a phased program that delivers quick wins early while building toward comprehensive security maturity.

Phase 1: Stop the Bleeding (Weeks 1-4)

Address all critical-risk items immediately. These are the controls whose absence creates direct, exploitable exposure:

- Deploy MFA on all externally accessible systems (email, VPN, cloud apps, RDP)
- Deploy managed EDR on all endpoints and servers
- Verify backup immutability: ensure at least one backup copy cannot be modified or deleted by ransomware
- Implement network segmentation for the most sensitive systems
- Block legacy authentication protocols
- Review and restrict email forwarding rules

Phase 2: Build the Foundation (Months 2-4)

Implement core security controls that provide broad protection:

- Deploy advanced email security with phishing protection and attachment sandboxing
- Implement DNS filtering to block known malicious domains
- Establish vulnerability scanning on a monthly cadence with defined remediation SLAs
- Document and test the incident response plan through a tabletop exercise
- Launch security awareness training program with quarterly phishing simulations
- Implement privileged access management for all administrative accounts

Phase 3: Mature and Automate (Months 5-8)

Build advanced capabilities and reduce manual effort:

- Deploy SIEM with centralized log collection and correlation rules
- Implement DLP policies for email, web, and cloud file sharing
- Deploy CSPM for continuous cloud configuration monitoring
- Automate access provisioning and deprovisioning through HR system integration
- Conduct external penetration test and remediate findings
- Establish formal vendor risk management program

Phase 4: Continuous Improvement (Ongoing)

- Conduct annual risk assessments and update control priorities
- Perform quarterly incident response tabletop exercises with rotating scenarios
- Track security metrics and report to executive leadership monthly
- Benchmark maturity against NIST CSF or CIS Controls framework annually
- Review and update this assessment every 12 months

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 cybersecurity assessment? Contact us.

Phone: 949.208.8800 | Toll Free: 800.733.7030

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