BLACKBOX INTELLIGENCE GROUP · FREE RESOURCE

Cyber Insurance & Ransomware Readiness Checklist

52 control items across the seven categories insurers and ransomware actors actually look at. Walk through it before your next renewal, audit, or board review.

NIST CSF | CIS v8 | SP 800-171 | Cyber Insurance

Veteran-owned · OSCP-led · MSP-friendly

How to Use This Checklist

Each item is phrased the way an underwriter or IR responder would phrase it. For every box you can't honestly check, capture it as a remediation item. The "evidence" column is what an insurer or assessor will ask to see — collect it as you go and your next renewal becomes a fill-in-the-blanks exercise.

Status legend: **[Y]** implemented · **[P]** partial / in progress · **[N]** not implemented

1. Identity & Access Controls

[ ]	MFA enforced for **all** users (no exceptions, no break-glass without compensating control)	Conditional access policy export, MFA report
[ ]	MFA enforced on remote access (VPN, RDP gateway, Citrix, M365)	Sign-in logs, gateway config
[ ]	Privileged accounts use phishing-resistant MFA (FIDO2/hardware token)	Authentication method registry
[ ]	Legacy / basic authentication is blocked tenant-wide	Auth policy report
[ ]	Admin accounts are separate from daily-use accounts	AD/Entra account inventory
[ ]	Privileged accounts reviewed quarterly; stale removed	Quarterly review log
[ ]	Just-in-time / PIM used for high-privilege roles where supported	PIM activation logs
[ ]	Conditional access blocks risky sign-ins (impossible travel, anonymous IPs)	CA policy export, risky sign-in report

2. Endpoint & EDR

[ ]	EDR (not just AV) deployed on **100%** of servers and workstations	EDR coverage report, gap list
[ ]	EDR alerts are triaged 24/7 by humans (in-house or managed)	SOC SLA, monthly triage stats
[ ]	Endpoint isolation / containment can be triggered remotely in < 30 min	Runbook, last drill record
[ ]	Critical patches deployed within 14 days; high within 30 days	Patch compliance dashboard
[ ]	End-of-life OS / software inventory is zero, or has documented compensating controls	EOL inventory
[ ]	Application allowlisting on servers handling sensitive data	Allowlist policy
[ ]	Local admin rights removed from standard users	Endpoint privilege report
[ ]	Endpoint protection tamper-resistant; uninstall requires SOC approval	Tamper-protection config

3. Backups & Recovery

[ ]	Backups follow 3-2-1 (or 3-2-1-1-0) — at least one offline / immutable copy	Backup architecture diagram
[ ]	Backups are isolated from the production domain (separate credentials, ideally separate identity provider)	Identity boundary doc
[ ]	Backup integrity / restore test performed at least quarterly	Restore test log
[ ]	Documented RTO and RPO targets per system tier	BIA / DR plan
[ ]	Ransomware-specific recovery playbook exists and has been tabletoped in last 12 months	Tabletop after-action
[ ]	Backup access uses MFA and is alerted on anomalous activity	Backup audit log
[ ]	Cloud SaaS data (M365, Google Workspace) is backed up to an independent system	SaaS backup contract

4. External Exposure & Network

[ ]	No RDP, SMB, Telnet, or database ports exposed directly to the internet	External scan report
[ ]	External attack surface scanned at least quarterly; new exposures triaged	Quarterly scan reports
[ ]	VPN access requires MFA; idle sessions auto-terminate	VPN config
[ ]	TLS certificates are valid, current, and use modern ciphers	TLS posture scan
[ ]	Network segmentation isolates critical systems / OT / payment / CUI from general LAN	Network diagram, VLAN map
[ ]	Firewall rules reviewed at least every 6 months; "any/any" rules removed	Firewall rule review log
[ ]	Public IPs and DNS records inventoried and owned by a named team	External asset inventory

5. Email & Phishing Defense

[ ]	SPF, DKIM, and DMARC published; DMARC at `p=quarantine` or `p=reject`	DMARC report
[ ]	Inbound mail uses attachment sandboxing & URL rewriting	Mail security tenant config
[ ]	External-sender warnings on inbound email	Mail rule export
[ ]	Auto-forwarding to external addresses is blocked or alerted	Anti-exfil policy
[ ]	Security-awareness training delivered at least annually with phishing simulations	Training attendance, sim results
[ ]	BEC / wire-fraud out-of-band verification policy in writing	Finance verification SOP
[ ]	Mailbox audit logging enabled; suspicious mailbox-rule creation alerts	Audit log sample

6. Logging, Monitoring & IR

[ ]	Centralized logging for endpoints, identity, network, and SaaS	SIEM / log architecture
[ ]	Logs retained at least 90 days (12 months for regulated workloads)	Retention policy
[ ]	Written incident response plan, last reviewed in < 12 months	IR plan PDF
[ ]	IR plan includes legal, insurer, regulator, and law-enforcement contacts	Notification matrix
[ ]	IR retainer or pre-arranged DFIR partner identified	Retainer agreement
[ ]	Tabletop exercise within last 12 months including leadership	Tabletop after-action
[ ]	Logs are write-protected / shipped off-host so attackers can't delete them	Log shipping config

7. Vendor & Supply Chain

[ ]	Inventory of all third parties with access to data or systems	Vendor inventory
[ ]	Vendor access is least-privilege, MFA-enforced, time-bound	Vendor access review
[ ]	Critical vendors provide SOC 2 / ISO 27001 / equivalent attestation annually	Vendor attestations
[ ]	MSP/IT provider contract clearly defines security responsibilities and notification timelines	MSP contract / SOR
[ ]	Software supply chain inventoried (key SaaS, OSS dependencies for any custom code)	SBOM / SaaS list
[ ]	Process to revoke vendor access within 24 hours of contract end	Offboarding SOP

How to Score Yourself

Total items: 52. Honest scoring is the point — overstating posture to an insurer is the fastest way to lose a claim.

- **45+ implemented** — strong posture; focus on the few "P" / "N" items and document evidence.
- **35–44** — typical for small organizations without dedicated security; you're insurable but renewal terms may tighten unless gaps close.
- **25–34** — material risk exposure; expect higher premiums, sublimits, or coverage exclusions on ransomware.
- **< 25** — most carriers will decline or require remediation before binding. Treat this as urgent.

Need a Hand?

If you marked "P" or "N" on more than ten items, the Security Reality Check is the right next step. We validate exposure across the same categories above and hand you a prioritized 30-day roadmap with evidence prompts already attached.

Book a 20-minute Security Fit Call: https://blackboxintelgroup.com/book-call