CENOVA CYBER
MANAGED SECURITY SERVICES

CYBER INSURANCE RENEWAL AUDIT

Security Controls Checklist | Annual Review

This checklist maps the 11 required CIS controls and operational policies that cyber insurers verify at renewal. All items must be fully implemented — not just planned — before attestation. Missing controls are the leading cause of denied claims and coverage gaps.

IDENTITY & ACCESS MANAGEMENT

- ☐ **Multi-Factor Authentication (MFA)** All remote and local admin accounts — CIS 6.4, 6.5
- ☐ **Access Control / Strong Password Policy** Unassociated account removal enforced — CIS 5.1, 5.2, 5.3

EMAIL & DOMAIN SECURITY

- ☐ **SPF, DKIM, DMARC Configured** All sending domains — CIS 9.5
- ☐ **Email Filtering Deployed** Inbound/outbound threat filtering — CIS 9.2, 9.3, 9.4

ENDPOINT PROTECTION

- ☐ **Next-Gen Antivirus (NGAV) Deployed** All endpoints — CIS 10.1
- ☐ **Endpoint Detection & Response (EDR)** Behavioral monitoring on all endpoints — CIS 13.7
- ☐ **Encryption on Endpoints & In Transit** Full-disk + data in transit — CIS 3.1, 3.11

NETWORK & REMOTE ACCESS

- ☐ **Secure Remote Access** VPN or zero-trust remote access — CIS 13.5
- ☐ **RDP and SMB Ports Blocked** Externally exposed ports closed — CIS 4.5

PATCHING & BACKUP

- ☐ **Patch Management Program Active** OS and application patches current — CIS 7.3
- ☐ **Backup — Min. 1 Online, 1 Offline with Testing** Tested recovery for on-prem and hybrid environments — CIS 11.2, 11.4

HUMAN RISK MANAGEMENT

☐	**Security Awareness Training (SAT)**	Annual minimum with documented completion — CIS 14.2
☐	**Phishing Simulation Training**	Quarterly simulations, not just at onboarding — CIS 14.2

📋 OPERATIONAL POLICIES & PROCEDURES

☐	**Written Incident Response Plan**	Documented and tested before an attack occurs
☐	**Dual Authorization for Wire Transfers**	Two-person approval above defined threshold
☐	**Call-Back Verification for Payment Changes**	Verified phone number — independent of email
☐	**Accurate Policy Representation at Renewal**	All attested controls must be fully in place

73%	58%	44%	$4.89M
of cyber incidents were BEC in 2024	of cyber claims were BEC or wire fraud	of claims denied for unmet requirements	avg. total breach cost with BEC compromise

COVERAGE GAPS TO CONFIRM WITH YOUR INSURER

☐ Social engineering / funds transfer fraud explicitly covered

☐ Notification cost sub-limits are adequate for your record count

☐ Regulatory defense coverage is sufficient

☐ Business interruption covers full recovery period

☐ Third-party / vendor breach exposure addressed

☐ 24–72-hour breach reporting requirement noted

INSURER ATTESTATION REMINDERS

All controls checked above must be fully deployed — not just planned — before attestation.

Report any incident or claim within 24–72 hours of discovery.

Review policy annually. Security posture changes can unlock premium savings of 30–40%.

Sources: FBI IC3 · Coalition 2025–2026 Cyber Claims Reports · Verizon DBIR 2025 · Sophos State of Ransomware 2025 · Hiscox · Industry Claims Report 2023. For informational purposes only. Consult your insurance broker and cybersecurity advisor.

Clarity, not Complexity

www.cenovacyber.com