Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

COMPLIANCE CHECKLIST — MID-MARKET PROFESSIONAL SERVICES

Cyber Insurance Readiness Checklist

15 Controls Carriers Require · Renewal Preparation · Application Accuracy

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

Cyber Insurance Readiness Checklist

About This Checklist

This checklist identifies the 15 security controls that cyber insurance carriers most frequently require, and most frequently cite as absent when denying or limiting claims. It was developed by analyzing carrier questionnaires from major cyber insurance providers including AIG, Chubb, Coalition, Corvus, At-Bay, Travelers, Beazley, and Munich Re, and mapping their common requirements to actionable implementation guidance.

Cyber insurance has undergone a fundamental transformation since 2020. What was once a largely unquestioned coverage has become a rigorously underwritten product with specific technical requirements. Premium increases of 30–200% have been common for organizations that cannot demonstrate basic controls, and outright coverage denials have increased significantly. More critically, carriers are increasingly scrutinizing claims and denying them based on misrepresentation — controls stated on the application that were not actually implemented at the time of the incident.

This checklist serves two purposes: it helps you prepare for renewal by identifying gaps before your carrier questionnaire is due, and it helps you accurately represent your security posture — protecting you from the coverage denial risk that misrepresentation creates.

Critical Warning

Cyber insurance applications ask whether specific controls are implemented. If you answer Yes to a control that is not actually in place and you subsequently file a claim arising from the absence of that control, your carrier may deny the claim and rescind the policy based on material misrepresentation. Complete this checklist before completing your application to ensure your answers are accurate.

How to Use This Checklist

Step 1 — Complete Before Your Application: Work through all 15 controls before completing your cyber insurance application or renewal questionnaire. Your application answers should match the status recorded here.

Step 2 — Score Honestly: Mark each control: Y (Yes — fully implemented and documented), P (Partial — something is in place but incomplete or inconsistently applied), or N (No — not implemented). P should be treated as N for insurance application purposes unless the partial implementation genuinely meets the carrier's intent.

Step 3 — Address Critical Gaps Before Renewal: Controls marked CRITICAL that are scored N or P represent your highest-priority remediation items. Most of these controls can be implemented in 30–60 days with appropriate support. Addressing them before renewal directly impacts your premium and coverage terms.

Step 4 — Document Everything: For each control implemented, document the evidence: policy document name and version, system configuration, vendor name, or screenshot of implementation. This documentation is what you provide if

a carrier requests verification.

THE 15 CONTROLS: CARRIER READINESS ASSESSMENT

Control 1: Multi-Factor Authentication (MFA) | Priority: CRITICAL

MFA is the single most-evaluated control in cyber insurance underwriting. Most carriers now treat MFA as a coverage condition — absence of MFA on email systems has been cited as grounds for claim denial in several publicized cases. MFA must be enforced (not merely available) on: all email accounts (including shared mailboxes), all cloud services, VPN and remote access, privileged and administrative accounts, and any system with financial transaction capability.

Implementation Guidance: *Microsoft 365: Azure AD Conditional Access > Require MFA. Google Workspace: 2-Step Verification enforcement via Admin Console. VPN: configure MFA requirement in your VPN management portal. Verify MFA is ENFORCED — not just enabled for some users.*

Status (Y / P / N): _____ Notes: _____

Control 2: Email Security — SPF, DKIM, DMARC | Priority: HIGH

Business email compromise (BEC) is the highest-dollar-loss cyber crime category. SPF, DKIM, and DMARC are the foundational technical controls that prevent email spoofing — the primary BEC attack vector. DMARC must be set to at minimum "quarantine" policy, with "reject" being the recommended final state. Many carriers now specifically ask about DMARC policy in applications.

Implementation Guidance: *Check current DMARC status: mxtoolbox.com/dmarc — enter your domain. If no DMARC record exists, this is your highest-priority email security remediation. Microsoft 365 includes SPF and DKIM setup in the Security & Compliance Center.*

Status (Y / P / N): _____ Notes: _____

Control 3: Endpoint Detection and Response (EDR) | Priority: HIGH

Traditional antivirus detects known malware signatures. Modern ransomware and advanced persistent threats are specifically designed to evade signature-based detection. EDR uses behavioral analysis to detect malicious activity regardless of whether the specific malware has been seen before. Carriers specifically distinguish between AV and EDR in underwriting — AV alone may result in a coverage limitation or surcharge for ransomware events.

Implementation Guidance: *Microsoft Defender for Business (included in M365 Business Premium at $22/user/month) provides EDR capability adequate for most mid-market organizations. CrowdStrike Falcon Go and SentinelOne Singularity Commercial are alternatives with broader platform support.*

Status (Y / P / N): _____ Notes: _____

Control 4: Privileged Access Management | Priority: HIGH

Privileged accounts — domain administrators, IT administrators, root accounts — are the primary lateral movement target in ransomware attacks. Once an attacker controls a privileged account, they can deploy ransomware across your entire environment. Privileged access management means: separate admin accounts from daily-use accounts (your IT person does not browse the web as a domain admin), MFA on all privileged accounts, quarterly review of who has privileged access, and immediate removal of access when an employee leaves.

Implementation Guidance: *Audit current privileged accounts: Active Directory > Users and Computers > Administrators group. Any account that is not actively needed as an administrator should be removed. Create separate named admin accounts for individuals who need privileged access, with MFA required.*

Status (Y / P / N): _____ Notes: _____

Control 5: Immutable or Offline Backups | Priority: CRITICAL

Ransomware operators specifically target backup systems before deploying the ransomware payload. If your backups are connected to your network and accessible with normal credentials, they will be encrypted alongside your production data. Immutable backups cannot be modified or deleted after they are written — they are ransomware-resistant by design. The 3-2-1 rule: 3 copies of data, on 2 different media types, with 1 copy offsite. All copies must be tested for restoration.

Implementation Guidance: *AWS Backup with Vault Lock, Azure Backup with immutability enabled, or Veeam with object lock. For smaller organizations: a physical external drive kept offsite (rotated weekly) combined with cloud backup provides offline protection. Test restoration from backup — monthly for critical systems, quarterly for all systems. Document test results.*

Status (Y / P / N): _____ Notes: _____

Control 6: Documented Incident Response Plan | Priority: HIGH

An incident response plan is not primarily a security document — it is a claims optimization document. Organizations with a tested IR plan before an incident occurs recover faster, spend less on incident response, and have better outcomes in carrier negotiations. The IR plan must include: who makes decisions (and who is the backup), when to engage your IR retainer firm, when and how to notify your cyber insurer (most policies have 72-hour notification requirements), regulatory notification requirements, and client/patient communication procedures.

Implementation Guidance: *At minimum, create a one-page emergency contact sheet that lists: IR firm name and 24/7 number, cyber insurer claims line, legal counsel, and key internal contacts. This alone is a significant improvement over no plan. A full IR plan should be developed with legal counsel and your insurer.*

Status (Y / P / N): _____ Notes: _____

Control 7: Security Awareness Training with Phishing Simulation | Priority: MEDIUM

Human error is the initial attack vector in 74%+ of security incidents. Phishing remains the dominant delivery mechanism for ransomware and credential theft. Security awareness training with phishing simulation testing is now a standard carrier requirement and reduces click rates significantly — from industry averages of 30%+ to under 5% in mature programs. Training must be documented individually — name, date, content, completion. Generic "the team watched a video" is not sufficient for audit purposes.

Implementation Guidance: *KnowBe4 (most widely deployed), Proofpoint Security Awareness, or Microsoft Attack Simulator (included in M365 Defender plans). Budget $20–40/user/year for a standalone platform. Run phishing simulations at least quarterly. Document click rates and training completion.*

Status (Y / P / N): _____ Notes: _____

Control 8: Patch Management Program | Priority: HIGH

Unpatched software vulnerabilities are the primary initial access vector for opportunistic ransomware attacks that scan the internet for known vulnerabilities. The most exploited vulnerabilities are typically 1–5 years old — not zero-days — because organizations fail to apply available patches. Critical patches must be applied within 30 days. End-of-life software (Windows 7, Server 2012, deprecated applications) must be identified, and a plan to remediate or compensate must be documented.

Implementation Guidance: *Enable Windows Update for Business for automated patch deployment. Implement a vulnerability scanner (Tenable Nessus, Qualys, or Rapid7 InsightVM) to identify unpatched systems. Check your external attack surface: Shodan.io search for your IP range reveals what external attackers see. Any critical or high-severity findings require immediate remediation.*

Status (Y / P / N): _____ Notes: _____

Control 9: Remote Desktop Protocol (RDP) Controls | Priority: CRITICAL

Exposed RDP is the single most common initial access vector for ransomware. Attackers scan the entire internet for open RDP ports (TCP 3389) — this takes minutes with modern scanning tools. If your RDP is exposed directly to the internet, it is being actively probed. Most carriers will not write cyber insurance for organizations with exposed RDP without a significant surcharge, and some will decline coverage entirely. If exposed RDP is discovered after an incident, it can be cited as material misrepresentation.

Implementation Guidance: *Check your exposure immediately: Shodan.io, type "port:3389" and your IP range or hostname. If you see results, block TCP 3389 at your firewall IMMEDIATELY. RDP should only be accessible through VPN with MFA. If RDP is not needed at all, disable the service on Windows workstations and servers: Services > Remote Desktop Services > Disabled.*

Status (Y / P / N): _____ Notes: _____

Control 10: Vendor and Third-Party Risk Management | Priority: MEDIUM

The majority of significant data breaches involve a third party — a vendor, supplier, or subcontractor with access to your systems or data. Carrier questionnaires increasingly ask about your vendor risk management program. At minimum, you need: an inventory of vendors with access to your systems or data, security questionnaires for high-risk vendors (completed annually), and contracts that include security requirements and breach notification obligations.

Implementation Guidance: *Create a vendor inventory listing: vendor name, what systems/data they access, when their contract renews, whether a BAA/DPA is in place, and last security review date. High-risk vendors (those with access to financial systems, client data, or production infrastructure) should complete an annual security questionnaire. Use the SIG (Standardized Information Gathering) questionnaire or a simplified version for smaller vendors.*

Status (Y / P / N): _____ Notes: _____

Control 11: Network Segmentation | Priority: MEDIUM

Network segmentation limits the blast radius of ransomware by preventing it from moving laterally from an infected workstation to critical systems. At minimum: guest WiFi must be isolated from your corporate network (separate SSID on a separate VLAN), financial and clinical systems should be on a separate VLAN from general workstations, and servers should not be directly reachable from workstations without firewall inspection.

Implementation Guidance: *For small organizations: configure your WiFi access points to create a separate guest SSID with network isolation enabled. For larger organizations: implement VLANs on your managed switches to segment finance, clinical, and server infrastructure from general workstations. Your firewall or next-gen firewall should enforce inter-VLAN routing rules.*

Status (Y / P / N): _____ Notes: _____

Control 12: Data Inventory and Classification | Priority: MEDIUM

Carrier applications ask what types of sensitive data you hold and in what volume. Accurate answers protect you from misrepresentation claims. More fundamentally, you cannot protect data you do not know you have. A data inventory identifies what sensitive data exists, where it is stored, who can access it, and how long it is retained — the foundation of both data protection and data minimization programs.

Implementation Guidance: *Conduct an annual data discovery exercise. Ask each business unit: what types of data do you create, store, or process? Where does it live (local drives, SharePoint, cloud apps)? Who can access it? Classify data into tiers: Restricted (SSNs, PHI, financial account numbers), Confidential (client data, legal matters), Internal (business data), and Public.*

Status (Y / P / N): _____ Notes: _____

Control 13: Accurate and Complete Insurance Application | Priority: CRITICAL

This is not a technical control — it is a legal obligation. Every question on your cyber insurance application must be answered accurately based on the actual state of your controls at the time of application. "We plan to implement MFA soon" is not the same as "MFA is implemented." Carriers are conducting post-incident investigations to verify application accuracy. Material misrepresentation — even unintentional — can result in claim denial and policy rescission. Use this checklist to verify the actual state of each control before completing your application.

Implementation Guidance: *Have your IT administrator or security consultant verify the status of each technical control in this checklist before completing your renewal application. Document the evidence for each control you claim as implemented. If your broker or agent completes the application on your behalf, review every answer before signing. You are liable for accuracy.*

Status (Y / P / N): _____ Notes: _____

Control 14: Social Engineering / Funds Transfer Fraud Coverage | Priority: MEDIUM

Business email compromise (BEC) and voice cloning fraud are now the highest-dollar-loss cyber crimes — exceeding ransomware in many years. Many cyber policies have sub-limits or exclusions for social engineering fraud that are dramatically lower than the headline policy limit. Verify your policy: what is the social engineering sub-limit? Does it cover CEO fraud (impersonation of leadership)? Does it cover voice cloning? Implement dual authorization for all wire transfers — verbal confirmation via a pre-established channel for any wire transfer, regardless of how the request was received.

Implementation Guidance: *Review your policy declarations page for: social engineering fraud coverage and sub-limit, funds transfer fraud coverage and sub-limit, telephone-enabled social engineering coverage. Implement wire transfer controls: all wire transfers over your threshold (suggest $5,000) require a callback verification to a pre-established number for the counterparty.*

Status (Y / P / N): _____ Notes: _____

Control 15: Security Logging and Monitoring | Priority: MEDIUM

Log retention is essential for incident investigation, regulatory compliance, and carrier-required forensics. Most carriers require minimum 90-day log retention; 12 months is the recommended standard. Logs must capture: user login and logout events, failed authentication attempts, administrative actions (account creation, permission changes), large data exports, and email gateway events. Without logs, incident response is severely hampered and regulatory notification timelines may be impossible to meet.

Implementation Guidance: *Microsoft 365: enable Unified Audit Log (Security & Compliance Center > Search > Audit log search). Ensure the audit log is enabled — it is not enabled by default. Set retention to 90 days minimum. Configure alerts for: repeated failed logins (brute force indicator), unusual email forwarding rules (compromise indicator), and bulk file access or download.*

Status (Y / P / N): _____ Notes: _____

RENEWAL READINESS SCORE

CRITICAL Controls (5 total): Y: ___ / P: ___ / N: ___

HIGH Controls (5 total): Y: ___ / P: ___ / N: ___

MEDIUM Controls (5 total): Y: ___ / P: ___ / N: ___

TOTAL IMPLEMENTED (Y): _____ / 15

Interpretation: 15 / 15 = Favorable underwriting. 12–14 / 15 = Standard terms likely. Below 12 = Expect premium increase or coverage restriction. Any CRITICAL control as N = High risk of denial or claim dispute.

Cyber Insurance Optimization Support

Cyber insurance optimization — implementing required controls, accurately completing applications, and positioning for favorable renewal terms — is a core component of all Axiom Sovereign vCISO retainers. We help you close gaps before renewal, answer questionnaires accurately, and communicate your security posture effectively to underwriters.

Schedule a cyber insurance readiness review: calendly.com/cmissimore-6zkc/30min

Email: info@axiomsovereign.com · **Web:** axiomsovereign.com