Cyber Insurance Questionnaire Cheat Sheet

A practical reference for Canadian SMBs (10-150 employees).

By Mike Pearlstein, CISSP
Founder & CEO, Fusion Computing | CISSP-led, founded 2012
Named in Canada's 50 Best Managed IT Companies 2024 & 2025
Published 2026-05-19

fusioncomputing.ca | contact@fusioncomputing.ca | (416) 566-2845
100 King St W, Suite 5700, Toronto, ON M5X 1C7

Cyber Insurance Questionnaire Cheat Sheet

Mapping Insurer Questions to CIS Controls v8.1

For Canadian SMBs facing 2026 renewal questionnaires

Authored by **Mike Pearlstein, CISSP** -- Founder and CEO, Fusion Computing Reviewed and last updated 2026-05-19 Named in **Canada's 50 Best Managed IT Companies 2024 & 2025**

Fusion Computing -- Toronto-based MSP, founded 2012, CISSP-led, serving 10-150 employee Canadian SMBs.

Page 2 -- Why cyber-insurance questionnaires are now functional security audits

A 2023 cyber-insurance renewal in Canada was a one-page form. A 2026 renewal is a forty-question audit, and underwriters now decline or surcharge applications that cannot evidence specific controls. The shift is not theoretical. Marsh, Aon, Gallagher, Burns & Wilcox, Coalition, At-Bay, and CFC have all standardized on questionnaires that map line-by-line to CIS Controls v8.1, NIST CSF 2.0, or the Center for Internet Security Implementation Group profile -- frequently all three. The same controls show up under different question phrasings, but the underlying evidence requirement is the same: produce a date, a system, a screenshot, or a policy document. "We have it" is no longer an acceptable answer.

For Canadian SMBs in the 10-150 employee range, the practical effect is brutal. Roughly half the questionnaires Fusion has reviewed in 2026 contain at least one control the firm cannot evidence on the day the broker sends the form. The result is a renewal surcharge of 25-60%, a sub-limit on ransomware, an exclusion on social-engineering loss, or an outright declination that forces a scramble to a substandard market. The fix is rarely a tooling problem. It is almost always an evidence-production problem: the controls exist, but nobody has compiled the dated proof an underwriter will accept. This cheat sheet maps the eighteen CIS Controls v8.1 to the questions underwriters actually ask, the evidence Fusion's stack produces against each, and the 30-day path to a clean "yes" on every line.

Pages 3-5 -- The mapping table: 18 CIS Controls v8.1

Control 1 -- Inventory and Control of Enterprise Assets

Typical insurer questions (verbatim): - "Do you maintain a current inventory of all hardware assets that connect to the corporate network, including remote and personal devices?" - "What percentage of your endpoints are managed by your IT provider's RMM platform?"

Evidence Fusion's stack produces: Dated NinjaOne (or Datto RMM) asset report exported per renewal cycle, showing 100% endpoint enrollment, last-checked-in timestamp, and operating-system inventory. Intune device-compliance report for mobile assets. Reconciliation log of unmanaged-device discovery scans.

Common "no" answer that triggers premium uplift or declination: "We think we know all our devices, but BYOD laptops aren't tracked." Underwriters read this as an undefined attack surface; expect a 15-25% surcharge and a sub-limit on remote-access loss.

30-day path to "yes": Deploy RMM agent to every device on a managed allowlist, enroll mobile devices in Intune, run a network-discovery scan against the corporate VLAN, and produce a dated reconciliation report that ties every MAC address to a known asset or a quarantine action.

Control 2 -- Inventory and Control of Software Assets

Typical insurer questions (verbatim): - "Do you maintain a current inventory of all authorized software running on enterprise assets?" - "How do you prevent unauthorized software (including unsanctioned SaaS) from being installed or used?"

Evidence Fusion's stack produces: RMM software-inventory report by device, M365 / Entra ID application-consent log, ThreatLocker (or equivalent) allowlist policy export, and Defender for Cloud Apps shadow-IT report.

Common "no" answer: "Staff install whatever they need to do their jobs." This is a top-three declination trigger in 2026. Insurers map it directly to ransomware-via-unsanctioned-tooling claims.

30-day path to "yes": Stand up an allowlist tool (ThreatLocker, Microsoft AppLocker, or equivalent) in audit-only mode, run a 14-day shadow-IT discovery sweep, publish a written software-request policy, and switch the allowlist to enforce mode for new installs.

Control 3 -- Data Protection

Typical insurer questions (verbatim): - "Is sensitive data encrypted at rest on endpoints, servers, and backup media?" - "Do you have a documented data-classification policy and applied controls based on sensitivity?"

Evidence Fusion's stack produces: BitLocker / FileVault deployment report from Intune, Microsoft Purview sensitivity-label deployment status, dated data-classification policy document, and backup-encryption attestation from the backup vendor.

Common "no" answer: "Our laptops are encrypted but we don't really classify data." Underwriters surcharge this 10-15% and add a sub-limit on data-restoration costs.

30-day path to "yes": Confirm BitLocker / FileVault on 100% of endpoints, deploy three Purview sensitivity labels (Public, Internal, Confidential), auto-apply Confidential to file types matching PII patterns, and publish the one-page data-classification policy.

Control 4 -- Secure Configuration of Enterprise Assets and Software

Typical insurer questions (verbatim): - "Do you apply a documented security baseline to all enterprise assets (CIS Benchmarks, Microsoft Security Baselines, or equivalent)?" - "Are administrative privileges restricted and just-in-time?"

Evidence Fusion's stack produces: Intune configuration-profile export aligned to CIS Level 1 baseline, Defender for Endpoint security-posture report, Entra ID Privileged Identity Management (PIM) activation log, and the firm's hardening-standard document.

Common "no" answer: "Everyone in the office runs as a local administrator." Top-three declination trigger. Underwriters read it as ransomware blast-radius unbounded.

30-day path to "yes": Apply Microsoft Security Baseline via Intune to all Windows devices, strip local-admin rights from standard users, deploy a privileged-access workstation pattern for IT staff, and enable PIM for all Entra ID role assignments.

Control 5 -- Account Management

Typical insurer questions (verbatim): - "How do you provision and de-provision user accounts, and what is your maximum offboarding time?" - "Do you have a documented process for managing service and shared accounts?"

Evidence Fusion's stack produces: HR-integrated joiner-mover-leaver workflow log (Entra ID lifecycle), dated quarterly access-review report, shared-mailbox inventory with assigned owners, and the offboarding runbook with named accountabilities.

Common "no" answer: "We get to terminated accounts when we remember." Insurer language: "inadequate offboarding control." Expect a surcharge plus a named exclusion on insider-loss coverage.

30-day path to "yes": Map the joiner-mover-leaver runbook, integrate the HR system (BambooHR, Humi, or equivalent) with Entra ID for automated provisioning, set a 24-hour offboarding SLA with monitoring, and conduct a one-off cleanup pass on dormant accounts.

Control 6 -- Access Control Management

Typical insurer questions (verbatim): - "Is multi-factor authentication enforced for all users on all remote-access, cloud, and email accounts?" - "Do you use conditional-access policies to restrict sign-ins by location, device compliance, or risk?"

Evidence Fusion's stack produces: Entra ID Conditional Access policy export, MFA-enforcement compliance report (100% of licensed users), legacy-protocol disablement attestation, and the named-administrator privileged-access policy document.

Common "no" answer: "Most people have MFA but a few executives opted out." This is the single most common declination trigger. There is no surcharge to opt out of -- MFA is now a precondition.

30-day path to "yes": Enforce MFA tenant-wide with no exceptions, disable legacy authentication protocols (POP3, IMAP, SMTP basic auth), publish a conditional-access policy that blocks sign-ins from non-Canadian IPs by default, and require compliant devices for cloud access.

Control 7 -- Continuous Vulnerability Management

Typical insurer questions (verbatim): - "How often do you scan for vulnerabilities, and what is your maximum time to patch critical (CVSS 9+) vulnerabilities?" - "Do you have a documented vulnerability-management program with named accountability?"

Evidence Fusion's stack produces: Monthly vulnerability-scan report (Defender for Endpoint vulnerability management, Qualys, or Nessus), dated patch-deployment compliance report from the RMM, exception register for unpatchable systems, and the vulnerability-management policy document.

Common "no" answer: "We patch when we can." Insurers read it as an undefined risk surface; expect 15-25% surcharge.

30-day path to "yes": Stand up a monthly vulnerability scan (Defender for Endpoint covers this on most stacks), set a 14-day patch SLA for critical vulnerabilities and 30 days for high, document an exception process for systems that cannot be patched, and publish the policy.

Control 8 -- Audit Log Management

Typical insurer questions (verbatim): - "Do you collect, retain, and review security audit logs across endpoints, servers, network devices, and cloud services?" - "What is your log-retention period?"

Evidence Fusion's stack produces: SIEM (Microsoft Sentinel, Huntress, or Blackpoint) log-ingestion report, 365-day retention attestation, dated SOC review notes, and the log-monitoring runbook.

Common "no" answer: "Our IT person checks logs if something seems wrong." Underwriters treat this as no detection capability and apply a ransomware sub-limit.

30-day path to "yes": Connect endpoint, M365, and firewall logs to a managed-detection-and-response

(MDR) provider with 24/7 SOC coverage, set log retention to a minimum of 365 days, and produce the monthly SOC summary report for the renewal packet.

Control 9 -- Email and Web Browser Protections

Typical insurer questions (verbatim): - "Do you have advanced email security (anti-phishing, attachment sandboxing, URL rewriting) on all inbound email?" - "Are DMARC, DKIM, and SPF enforced on your sending domain?"

Evidence Fusion's stack produces: Microsoft Defender for Office 365 (or Proofpoint, Mimecast) policy export, DMARC report with p=reject, DKIM signature attestation, and the monthly phish-block summary.

Common "no" answer: "We have basic Office 365 email." If Defender for O365 Plan 1 or higher is not enabled, expect a surcharge on business-email-compromise coverage and a low sub-limit on social-engineering loss.

30-day path to "yes": Upgrade to Microsoft 365 Business Premium (which includes Defender for O365 Plan 1), publish DMARC at p=reject after a 30-day monitoring phase, validate DKIM signing, and enable Safe Attachments / Safe Links policies.

Control 10 -- Malware Defenses

Typical insurer questions (verbatim): - "Do you deploy endpoint detection and response (EDR) with active 24/7 monitoring on every endpoint and server?" - "Is your antivirus / EDR managed by a security operations centre?"

Evidence Fusion's stack produces: EDR coverage matrix from Defender for Endpoint (or SentinelOne, Huntress, CrowdStrike), 24/7 SOC monitoring contract, monthly detection-and-response report, and the incident-response playbook.

Common "no" answer: "We have antivirus but nobody watches it overnight." This is now a renewal precondition for ransomware coverage at standard rates.

30-day path to "yes": Deploy Defender for Endpoint Plan 2 (or equivalent) to 100% of endpoints and servers, engage a managed-detection-and-response provider with 24/7 SOC coverage, and run a tabletop exercise to validate the response runbook.

Control 11 -- Data Recovery

Typical insurer questions (verbatim): - "Do you perform daily backups of critical systems, and are backups stored immutably or air-gapped?" - "When did you last test a full restore, and was it successful?"

Evidence Fusion's stack produces: Datto / Veeam / Cove backup-completion log, immutability attestation from the backup platform, dated restore-test report (quarterly minimum), and the documented Recovery Time Objective (RTO) / Recovery Point Objective (RPO) per system tier.

Common "no" answer: "We have backups but we haven't tested them this year." Insurers treat untested backups as no backups. Expect a sub-limit on business-interruption coverage.

30-day path to "yes": Validate that backups exist for all production systems, confirm immutability is enabled at the storage layer, run a documented restore test against a critical system, and capture the dated success report for the renewal file.

Control 12 -- Network Infrastructure Management

Typical insurer questions (verbatim): - "Is your network segmented to isolate critical systems, guest devices, and operational technology?" - "Are network devices (firewalls, switches, access points) running

supported firmware and configured against a documented baseline?"

Evidence Fusion's stack produces: Network topology diagram, firewall configuration export (Fortinet, Sophos, Meraki, or equivalent), VLAN segmentation report, and the dated firmware-currency attestation.

Common "no" answer: "Our network is flat -- everything's on one VLAN." This is a top-five declination trigger for firms above 25 staff. The underwriter cannot price ransomware lateral-movement risk.

30-day path to "yes": Build a target topology with at least three segments (corporate, guest, server), reconfigure switches and firewalls to enforce the segmentation, validate firmware currency across all network devices, and document the topology diagram for the renewal packet.

Control 13 -- Network Monitoring and Defense

Typical insurer questions (verbatim): - "Do you have network-traffic monitoring and alerting in place to detect anomalous behaviour?" - "Is there 24/7 monitoring by a security operations centre or managed-detection-and-response provider?"

Evidence Fusion's stack produces: MDR provider engagement letter and SOC coverage attestation, monthly detection-summary report, network-IDS / firewall-log ingestion confirmation, and the documented escalation path.

Common "no" answer: "We get alerts but nobody's on call after hours." Underwriters apply a ransomware sub-limit because mean-time-to-detect exceeds attacker dwell time.

30-day path to "yes": Engage a 24/7 SOC / MDR provider (Huntress, Blackpoint, Arctic Wolf, or equivalent), connect firewall and endpoint telemetry, and validate the escalation path with a documented test alert.

Control 14 -- Security Awareness and Skills Training

Typical insurer questions (verbatim): - "Do all employees complete security awareness training at hire and at least annually?" - "Do you run simulated phishing campaigns and track click rates and reporting rates?"

Evidence Fusion's stack produces: Training-platform completion report (KnowBe4, Hoxhunt, or equivalent), phishing-simulation results report with click and report rates by quarter, and the security-awareness program policy document.

Common "no" answer: "We tell people to be careful with email." Underwriters apply a social-engineering sub-limit. The named cost is real: business-email-compromise loss can exceed the policy limit if training is absent.

30-day path to "yes": Roll out KnowBe4 (or equivalent) to 100% of staff, assign the new-hire onboarding module, run a baseline phishing simulation, and schedule quarterly campaigns going forward.

Control 15 -- Service Provider Management

Typical insurer questions (verbatim): - "Do you maintain an inventory of third-party service providers with access to your data or systems, including their SOC 2 attestation status?" - "Do you have a documented vendor-risk management process?"

Evidence Fusion's stack produces: Vendor inventory with data-class classification, SOC 2 Type II reports for in-scope vendors (or equivalent attestations), Data Processing Agreements on file, and the dated quarterly vendor-review log.

Common "no" answer: "We don't track vendors that touch our data." Underwriters surcharge this 10-15% and may exclude supply-chain loss.

30-day path to "yes": Build the vendor inventory (most SMBs land between 12 and 30 vendors), request SOC 2 Type II from any vendor that touches client data, document a residual-risk decision for vendors that cannot produce one, and schedule the next review. See Fusion's CIRO Third-Party-Risk Evidence Template (page 18523) for a reusable structure.

Control 16 -- Application Software Security

Typical insurer questions (verbatim): - "Do you maintain an inventory of business applications and confirm vendor security posture for SaaS applications you depend on?" - "Do you perform secure-configuration reviews on critical applications?"

Evidence Fusion's stack produces: SaaS application inventory with admin-console review notes, Microsoft Secure Score report, Defender for Cloud Apps risk-assessment report, and the dated configuration-review log.

Common "no" answer: "We use whatever SaaS our staff signed up for." Underwriters apply the same surcharge as Control 15 (vendor inventory) plus a sub-limit on SaaS-related data loss.

30-day path to "yes": Audit the M365 application-consent log, baseline Microsoft Secure Score (target ? 60%), document the admin-console configuration of the top five SaaS dependencies, and publish the SaaS-governance policy.

Control 17 -- Incident Response Management

Typical insurer questions (verbatim): - "Do you have a written incident-response plan with named roles, decision trees, and external-counsel contacts?" - "When did you last conduct a tabletop exercise, and what were the after-action findings?"

Evidence Fusion's stack produces: Documented incident-response runbook with named on-call lead, decision tree, and breach-counsel contact information; dated tabletop-exercise report; CRA / Office of the Privacy Commissioner / provincial regulator notification template; and the post-incident reporting log.

Common "no" answer: "We'd figure it out if something happened." Underwriters apply a sub-limit on incident-response coverage and may require the firm to use the insurer's panel breach-counsel firm at preferred rates.

30-day path to "yes": Write a one-page incident-response runbook, name the on-call lead and a backup, engage breach-counsel and a digital-forensics-and-incident-response (DFIR) firm in advance, run a 90-minute tabletop exercise on a ransomware scenario, and capture the after-action notes.

Control 18 -- Penetration Testing

Typical insurer questions (verbatim): - "Have you conducted a penetration test in the last twelve months, and were the findings remediated?" - "Is the penetration testing scope documented and aligned to your risk profile?"

Evidence Fusion's stack produces: Annual external penetration test report from an independent provider, remediation log mapped to findings, and the scope-of-work document for the next test.

Common "no" answer: "We've never had a pen test." For firms above 50 staff or with regulated data, this is increasingly a precondition for cyber-insurance limits above $1M. Below 50 staff, vulnerability scans plus an external-attack-surface assessment can substitute, but the underwriter will document the substitution.

30-day path to "yes": Scope an external-network penetration test with an independent CREST- or OSCP-certified provider, schedule the test, agree the remediation timeline in advance, and budget for one annual test going forward. Smaller firms can run an external-attack-surface scan (Censys, Shodan, or vendor-provided) as a bridge.

Page 6 -- Next steps

The pattern Fusion sees

Of the cyber-insurance questionnaires we have walked through with Canadian SMBs in 2026, roughly two-thirds contain at least one control the firm can implement inside 30 days but does not yet evidence. The cost of fixing the evidence gap is almost always smaller than a single year's renewal surcharge. The cost of an outright declination -- and the scramble to a substandard carrier with sub-limits and exclusions -- is materially larger than any of the implementation lifts in this cheat sheet.

Walk the questionnaire with us

The most useful service Fusion provides at renewal time is also the simplest: we sit with your broker and your operations lead and walk the questionnaire question-by-question against the evidence we already produce for you. For prospective clients, the equivalent is a 60-minute working session where we map your current stack against the eighteen controls above, identify the gaps in evidence (not necessarily controls -- most firms have more in place than they think), and produce a 30-day path to a clean "yes" on every line that matters for your renewal.

The session is no-charge. There is no expectation that you move IT providers to qualify. Bring the questionnaire and the renewal date.

Book a session

Visit **fusioncomputing.ca/contact-us/** and choose a 60-minute working session on the calendar. Reference "cyber-insurance walkthrough" in the form.

We will sit with your broker to walk the questionnaire together.

Fusion Computing -- Toronto-based MSP, founded 2012. CISSP-led. Serving Canadian SMBs across managed IT, cybersecurity, Microsoft 365, and cyber-insurance evidence production. Named in Canada's 50 Best Managed IT Companies 2024 & 2025.

This cheat sheet is a practitioner-built consolidation. It is not legal advice and is not a substitute for your insurance broker's professional judgement or the underwriter's authoritative questionnaire. CIS Controls v8.1 is a trademark of the Center for Internet Security. Sources: cisecurity.org, marsh.com, coalitioninc.com, atbay.com, ciso.gov, csc.gc.ca/cybersecurity.