2026 Canadian SMB IT & Security Readiness Checklist

A 15-Minute Self-Assessment Aligned to CIS Controls v8.1

12 categories | 78 controls | Actionable next steps
For owners, office managers, and IT leads at Canadian businesses with 10-150 employees

Prepared by **Mike Pearlstein, CISSP** - CEO, Fusion Computing Limited
fusioncomputing.ca | (416) 566-2845 | March 2026
Toronto | Hamilton | Metro Vancouver

How to Use This Checklist

This checklist is a practical self-assessment for Canadian small and medium businesses. It covers 12 categories aligned to the CIS Controls v8.1 framework, a widely adopted set of cybersecurity best practices used by organizations of all sizes across North America.

For each control, mark the **Yes**, **No**, or **N/A** circle. Be honest. This is a diagnostic tool, not a compliance audit. The goal is to identify gaps so you can prioritize improvements.

Quick scoring guide: Count your Yes answers across all 78 controls. **65-78 = Strong** | **45-64 = Developing** | **25-44 = At Risk** | **0-24 = Critical** Full scoring guide on the last pages.

Who should complete this?

Ideally, your IT lead, office manager, or whoever is responsible for technology decisions. If you have an MSP, complete it together. A good MSP should be able to answer every question immediately. If they cannot, that is a finding in itself.

A note on frameworks

This checklist maps to CIS Controls v8.1 Implementation Group 1 (IG1), which represents the essential cyber hygiene that every organization should implement regardless of size. Some items extend into IG2 where they are particularly relevant to Canadian compliance requirements (PIPEDA, provincial privacy laws, cyber insurance underwriting).

Categories

01 Asset Inventory & Management (CIS Control 1 & 2)
02 Data Protection & Classification (CIS Control 3)
03 Access Control & Identity (CIS Control 5 & 6)
04 Endpoint Protection (CIS Control 4 & 10)
05 Email Security (CIS Control 9)
06 Network Security (CIS Control 9 & 12)
07 Backup & Disaster Recovery (CIS Control 11)
08 Security Awareness & Training (CIS Control 14)
09 Vulnerability & Patch Management (CIS Control 7)
10 Incident Response & Logging (CIS Control 8 & 17)
11 Cloud & Microsoft 365 Security (CIS Control 3 & 6)
12 Governance, Policy & Compliance (CIS Control 15 & 16)

01 Asset Inventory & Management (CIS Control 1 & 2)

You cannot protect what you do not know about. This category covers whether your business maintains a current, accurate inventory of all hardware and software, and whether unauthorized assets are detected.

Control	Yes	No	N/A
We maintain a current inventory of all hardware assets (workstations, servers, network devices, mobile devices)	[ ]	[ ]	[ ]
We maintain a current inventory of all software installed across the organization	[ ]	[ ]	[ ]
We have a process to detect and flag unauthorized devices connecting to our network	[ ]	[ ]	[ ]
We have a process to detect and flag unauthorized or unapproved software	[ ]	[ ]	[ ]
Asset inventory is reviewed and updated at least quarterly	[ ]	[ ]	[ ]
End-of-life hardware and unsupported software are tracked and scheduled for replacement	[ ]	[ ]	[ ]
All assets are assigned an owner responsible for their maintenance and security	[ ]	[ ]	[ ]

Why this matters: Untracked assets are invisible to security tools. In Fusion's onboarding assessments, stale admin accounts on forgotten hardware are one of the most common findings. A single unpatched laptop or decommissioned server is often the entry point for a breach.

02 Data Protection & Classification (CIS Control 3)

Knowing where your sensitive data lives and how it is protected is fundamental. This covers data classification, encryption, and data loss prevention.

Control	Yes	No	N/A
We have a documented data classification policy (e.g. public, internal, confidential, restricted)	[ ]	[ ]	[ ]
Sensitive data at rest is encrypted (laptops, servers, cloud storage)	[ ]	[ ]	[ ]
Sensitive data in transit is encrypted (TLS/HTTPS enforced, VPN for remote access)	[ ]	[ ]	[ ]
We know which cloud services store our data and where that data is geographically located	[ ]	[ ]	[ ]
We have data loss prevention (DLP) controls to prevent accidental sharing of sensitive data	[ ]	[ ]	[ ]
Former employee access to company data is revoked within 24 hours of departure	[ ]	[ ]	[ ]

Why this matters: Under PIPEDA and evolving federal and provincial privacy legislation, Canadian businesses have specific obligations around how personal information is collected, stored, and disclosed. A breach involving unencrypted data carries both regulatory and reputational risk.

03 Access Control & Identity (CIS Control 5 & 6)

Who can access what, and how is that access verified? This covers identity management, multi-factor authentication, and the principle of least privilege.

Control	Yes	No	N/A
Multi-factor authentication (MFA) is enforced on all user accounts (email, VPN, cloud apps)	[ ]	[ ]	[ ]
Admin/privileged accounts use separate credentials from day-to-day user accounts	[ ]	[ ]	[ ]
We follow the principle of least privilege: users only have access to what they need	[ ]	[ ]	[ ]
Access permissions are reviewed at least annually	[ ]	[ ]	[ ]
We have a documented process for onboarding and offboarding user accounts	[ ]	[ ]	[ ]
Shared accounts and shared passwords are prohibited or actively being eliminated	[ ]	[ ]	[ ]
Password policy enforces minimum 14 characters or passphrase requirements	[ ]	[ ]	[ ]

Why this matters: Compromised credentials are the leading attack vector for Canadian SMBs. Microsoft reports that MFA blocks more than 99% of automated account compromise attempts. In our client environments, enforcing MFA is consistently the single highest-impact security improvement.

04 Endpoint Protection (CIS Control 4 & 10)

Every workstation, laptop, and server is a potential entry point. This covers whether your endpoints are hardened, monitored, and consistently configured.

Control	Yes	No	N/A
All endpoints run a managed endpoint detection and response (EDR) solution, not just traditional antivirus	[ ]	[ ]	[ ]
Operating system patches are applied within 14 days of release for critical vulnerabilities	[ ]	[ ]	[ ]
Application patches (browsers, PDF readers, Java, etc.) are applied within 30 days	[ ]	[ ]	[ ]
Endpoints are configured using a security baseline (e.g. CIS Benchmarks, Microsoft Security Baselines)	[ ]	[ ]	[ ]
USB storage and removable media are restricted or monitored	[ ]	[ ]	[ ]
Screen lock is enforced after 5 minutes of inactivity	[ ]	[ ]	[ ]
Full disk encryption is enabled on all laptops and mobile devices	[ ]	[ ]	[ ]

Why this matters: An unpatched endpoint is an open door. The window between vulnerability disclosure and active exploitation continues to shrink, with many critical vulnerabilities being exploited within days of public disclosure.

05 Email Security (CIS Control 9)

Email remains the primary attack vector for phishing, business email compromise (BEC), and malware delivery. This covers your technical and human defences.

Control	Yes	No	N/A
SPF, DKIM, and DMARC are configured and enforced on all company domains	[ ]	[ ]	[ ]
DMARC policy is set to quarantine or reject (not just monitor/none)	[ ]	[ ]	[ ]
Advanced threat protection / safe links / safe attachments are enabled	[ ]	[ ]	[ ]
External email tagging is enabled (banners warning users of external senders)	[ ]	[ ]	[ ]
Employees receive phishing simulation training at least quarterly	[ ]	[ ]	[ ]
A clear process exists for employees to report suspicious emails	[ ]	[ ]	[ ]
An email retention and archival policy is in place for business and compliance purposes	[ ]	[ ]	[ ]

Why this matters: The vast majority of successful cyberattacks start with a phishing email. DMARC at enforcement prevents domain spoofing, yet most Canadian SMBs still run DMARC in monitor-only mode. When Fusion onboards a new client, a misconfigured or missing DMARC record is one of the first things we check.

06 Network Security (CIS Control 9 & 12)

Your network is the connective tissue. This covers firewall management, segmentation, DNS filtering, and wireless security.

Control	Yes	No	N/A
A business-grade firewall with active threat intelligence subscription is in place	[ ]	[ ]	[ ]
Firewall firmware is updated within 30 days of critical patches	[ ]	[ ]	[ ]
Network segmentation separates critical systems from general user traffic	[ ]	[ ]	[ ]
Guest Wi-Fi is isolated from the corporate network	[ ]	[ ]	[ ]
DNS filtering is enabled to block known malicious domains	[ ]	[ ]	[ ]
Remote access uses a VPN or zero-trust network access (ZTNA) solution	[ ]	[ ]	[ ]
Default credentials on network equipment have been changed	[ ]	[ ]	[ ]

Why this matters: A flat network means one compromised device gives an attacker access to everything. Segmentation limits lateral movement and contains incidents.

07 Backup & Disaster Recovery (CIS Control 11)

When everything else fails, backups are your last line of defence. This covers backup strategy, testing, and recovery planning.

Control	Yes	No	N/A
All critical data and systems are backed up automatically on a documented schedule	[ ]	[ ]	[ ]
Backups follow the 3-2-1 rule (3 copies, 2 media types, 1 offsite/cloud)	[ ]	[ ]	[ ]
At least one backup copy is air-gapped or immutable (cannot be modified by ransomware)	[ ]	[ ]	[ ]
Backup restoration is tested at least quarterly with documented results	[ ]	[ ]	[ ]
Recovery time objectives (RTO) and recovery point objectives (RPO) are defined and documented	[ ]	[ ]	[ ]
A written disaster recovery plan exists and has been reviewed in the past 12 months	[ ]	[ ]	[ ]

Why this matters: Backups that have never been tested are not backups. They are assumptions. Fusion has recovered clients from active ransomware incidents without paying because tested, immutable backups were already in place. The difference between paying a ransom and recovering cleanly almost always comes down to whether the backups were tested.

08 Security Awareness & Training (CIS Control 14)

Your employees are both your greatest vulnerability and your strongest defence. This covers ongoing security education and culture.

Control	Yes	No	N/A
All employees complete cybersecurity awareness training during onboarding	[ ]	[ ]	[ ]
Ongoing security training is delivered at least annually (ideally quarterly)	[ ]	[ ]	[ ]
Phishing simulations are conducted regularly with tracked results	[ ]	[ ]	[ ]
Employees know how to report suspicious activity (clear escalation path)	[ ]	[ ]	[ ]
Training covers social engineering, BEC fraud, and safe browsing, not just phishing	[ ]	[ ]	[ ]
Leadership participates in training (sets the tone from the top)	[ ]	[ ]	[ ]

Why this matters: Technical controls catch known attacks. Trained employees catch everything else. CIRA's 2025 Cybersecurity Survey found that 43% of Canadian organizations were targeted by a cyber attack in the past year (source).

09 Vulnerability & Patch Management (CIS Control 7)

Finding and fixing vulnerabilities before attackers exploit them. This covers scanning, prioritization, and remediation timelines.

Control	Yes	No	N/A
Vulnerability scans are run at least monthly across all internal and external-facing systems	[ ]	[ ]	[ ]
Critical vulnerabilities (CVSS 9.0+) are remediated within 72 hours	[ ]	[ ]	[ ]
High vulnerabilities (CVSS 7.0-8.9) are remediated within 30 days	[ ]	[ ]	[ ]
Third-party applications are included in the patching program (not just OS patches)	[ ]	[ ]	[ ]
A patch management policy with defined SLAs exists and is followed	[ ]	[ ]	[ ]
Vulnerability scan results are reviewed by a senior technician, not just auto-closed	[ ]	[ ]	[ ]

Why this matters: The window between disclosure and exploitation is shrinking. Automated patching covers the basics, but prioritized remediation of critical vulnerabilities is what prevents breaches.

10 Incident Response & Logging (CIS Control 8 & 17)

When something goes wrong, how fast can you detect, contain, and recover? This covers logging, monitoring, and your incident response plan.

Control	Yes	No	N/A
Security event logs are collected from all critical systems (servers, firewalls, endpoints, cloud)	[ ]	[ ]	[ ]
Logs are retained for at least 90 days (180+ days recommended)	[ ]	[ ]	[ ]
Logs are monitored for anomalies, either by staff or a managed detection service	[ ]	[ ]	[ ]
A written incident response plan exists with defined roles and communication procedures	[ ]	[ ]	[ ]
The incident response plan has been tested (tabletop exercise or simulation) in the past 12 months	[ ]	[ ]	[ ]
We have a relationship with an incident response provider or our MSP includes IR in our contract	[ ]	[ ]	[ ]

Why this matters: Organizations without centralized logging often take months to detect a breach. Centralized monitoring and a tested incident response plan can reduce that to hours. An untested incident response plan is just a document.

11 Cloud & Microsoft 365 Security (CIS Control 3 & 6)

Most Canadian SMBs run on Microsoft 365. This covers whether your cloud environment is configured securely or running on out-of-box defaults.

Control	Yes	No	N/A
Microsoft 365 Secure Score has been reviewed and is above 60%	[ ]	[ ]	[ ]
Conditional access policies are configured (location, device compliance, risk-based)	[ ]	[ ]	[ ]
Legacy authentication protocols are disabled in M365	[ ]	[ ]	[ ]
Audit logging is enabled in Microsoft 365 (not enabled by default on all plans)	[ ]	[ ]	[ ]
SharePoint/OneDrive external sharing is restricted to approved domains or disabled	[ ]	[ ]	[ ]
Admin accounts in M365 use dedicated admin-only identities with MFA	[ ]	[ ]	[ ]

Why this matters: Microsoft 365 out of the box is not secure. Default settings prioritize collaboration over security. Conditional access and audit logging are table-stakes configurations that most SMBs skip. Fusion configures these as part of every onboarding.

12 Governance, Policy & Compliance (CIS Control 15 & 16)

Security is not just technical. It is organizational. This covers whether your business has the policies, accountability, and compliance documentation to back up your technical controls.

Control	Yes	No	N/A
An acceptable use policy (AUP) exists and is signed by all employees	[ ]	[ ]	[ ]
A cybersecurity policy or information security policy exists and is reviewed annually	[ ]	[ ]	[ ]
Privacy obligations under PIPEDA (and applicable provincial laws) are documented and followed	[ ]	[ ]	[ ]
Cyber insurance is in place and the policy has been reviewed in the past 12 months	[ ]	[ ]	[ ]
A named individual (internal or external vCISO) is accountable for cybersecurity	[ ]	[ ]	[ ]
Vendor and third-party risk is assessed before granting access to systems or data	[ ]	[ ]	[ ]
Board or leadership receives a security posture report at least annually	[ ]	[ ]	[ ]

Why this matters: Insurers, clients, and regulators increasingly ask for evidence of documented security governance. Having the controls without the documentation is almost as risky as having neither.

If You Scored Below 45: Start Here

These five controls deliver the highest risk reduction per dollar. If your assessment revealed significant gaps, prioritize these before anything else.

#	Action	Why it matters most
1	**Enforce MFA on every account**	Blocks more than 99% of automated credential attacks. Highest single-control impact. Start with admin accounts, then all users.
2	**Test your backups — today**	Verify at least one restore to bare metal or clean VM. If the restore fails, you do not have a backup. You have a file.
3	**Set DMARC to quarantine or reject**	Prevents attackers from sending email as your domain. Most Canadian SMBs still run DMARC in monitor-only mode, which provides visibility but no protection.
4	**Deploy EDR on every endpoint**	Traditional antivirus misses modern threats. EDR provides behavioural detection, remote isolation, and forensic visibility that AV cannot.
5	**Disable legacy authentication in M365**	Legacy auth protocols bypass MFA entirely. Disabling them closes one of the most common M365 attack paths with zero user-facing impact for modern clients.

These five controls are drawn from CIS IG1 and represent the consensus starting point recommended by Fusion's security team for businesses scoring in the At Risk or Critical range.

Score Your Results

Count the total number of **Yes** answers across all 12 categories (78 controls total).

65-78	**Strong**	Your security fundamentals are solid. Focus on maintaining controls, testing assumptions (especially backup restoration and incident response plans), and advancing to IG2 controls.
45-64	**Developing**	You have a foundation but meaningful gaps remain. Prioritize access control (MFA everywhere), endpoint protection, and backup verification.
25-44	**At Risk**	Significant gaps exist across multiple categories. Start with the five Quick Wins on the previous page, then build a prioritized remediation plan.
0-24	**Critical**	Minimal security controls are in place. Every day without action increases exposure. Start with the five Quick Wins, then get a professional assessment.

This checklist covers CIS Controls IG1 (essential cyber hygiene). A comprehensive assessment would also evaluate penetration testing, supply chain risk, and regulatory compliance specific to your industry.

What to Do With Your Results

This checklist gives you a snapshot. A strategy gives you a plan.

Your score	Recommended next step
Strong (65-78)	Book a vCISO strategy session to advance to CIS IG2 and prepare for compliance audits, insurance renewals, or client security questionnaires.
Developing (45-64)	Book a free 30-minute consultation to review your gaps and build a prioritized 90-day remediation roadmap. No obligation.
At Risk (25-44)	Book a complimentary IT and Security Assessment. Fusion reviews your infrastructure, security posture, and operational readiness, then delivers a written report with prioritized recommendations.
Critical (0-24)	Call us directly at (416) 566-2845. We can help you prioritize the most urgent gaps and build a stabilization plan.

Book a Free Strategy Call

calendly.com/fusioncomputing/technology-health-check

Fusion Computing Limited
100 King Street West, Suite 5700, Toronto, ON M5X 1C7
Sales: (416) 566-2845 | fusioncomputing.ca | sales@fusioncomputing.ca

CISSP-Certified Leadership | CIS Controls v8.1 Aligned | Since 2012 | Canadian-Owned

This checklist is provided for educational purposes and does not constitute legal, regulatory, or professional security advice. CIS Controls is a registered trademark of the Center for Internet Security, Inc. Fusion Computing Limited is not affiliated with CIS. Assessment results should be validated by a qualified security professional before making compliance or investment decisions.