FEBRUARY 2026

DATARISK
CANADA

CCCS Recommended Cyber Security Contract

Vendor Contract Risk Management Checklist for Canadian SMEs

A readiness tool for vendor risk assessments, supply-chain security, and contract negotiation

Prepared by Datarisk Canada

Based on ‘Recommended cyber security contract clauses for cloud services’ by the Canadian Center of Cyber Security

Table of Contents

The **Canadian Centre for Cyber Security (the Cyber Centre)** is part of the Communications Security Establishment Canada. It is the single unified source of expert advice, guidance, services and support on cyber security for Canadians.

1. Purpose and intended audience

This document is intended to build upon the guidance of the Cyber Centre with a check-list based exercise. It also helps Canadian small and mid-size enterprises (SMEs) manage cybersecurity and privacy risk when contracting with:

- **Cloud Service Providers (CSPs)**
- **Managed Security Service Providers (MSSPs)**
- **AI vendors (including SaaS products that embed AI features)**

It is designed for **IT leads and compliance leads** who are responsible for vendor onboarding, renewal, and vendor risk assessment. It converts common contract risk areas into **clear, prescriptive questions** that can be used to:

- Find and assess contract language
- Identify gaps
- Negotiate targeted improvements
- Document risk acceptance when necessary.

2. When to use this checklist

Use this checklist in any of the following situations:

New vendors (pre-signature)

- RFP/RFI, procurement reviews, onboarding security reviews
- Contract negotiations (MSA + SOW + DPA + security exhibit)

Existing vendors (post-signature)

- Renewal, scope expansion, migration, or new data types/workloads
- After an incident, near miss, or audit finding
- When the vendor adds AI features, new subprocessors, or new regions

Ongoing vendor governance

- Annual/biannual vendor risk reviews
- Evidence collection for audits, insurance, or customer due diligence

3. How to use this checklist in real vendor engagements

Datarisk Canada recommends the following workflow:

1. **Confirm the vendor type(s):** CSP, MSSP, AI vendor (many are multiple).

2. **Gather the complete contract stack:** MSA, SOW, DPA, security exhibit, acceptable use policy, and any incorporated online terms.

3. **Run the Core 12 first** (Section 4.1)

4. **Record evidence beside each answer** (clause references, URLs, exhibit names, or screenshots).

5. **Classify outcomes:**
   - Meets: clear, enforceable, aligned with your needs
   - Partial: present but unclear, limited, or requires a paid tier
   - No: absent or unacceptable
   - N/A: not applicable to this vendor/service

6. **Resolve gaps by approach:**
   - Contract edits (preferred for critical risks)
   - Security schedule addendum / DPA updates
   - SOW commitments (often negotiable even when MSAs are rigid)
   - Compensating controls (when negotiation is not feasible)

7. **Escalate Stop/Go triggers to executive sign-off** (Section 4.2)

4. The 80/20 priorities

4.1 The Core 12 (first 30–60 minutes)

These are the areas that most often drive real-world harm: unauthorized data use, delayed incident response, opaque third parties, lock-in, and one-way liability. If time and negotiation leverage are limited, start here.

Data control and misuse prevention

- [ ] **Data use limitation:** Is the vendor restricted to using your data only to deliver the service (no secondary use)?
- [ ] **AI training prohibition (opt-in only):** Is the vendor prohibited from using your data to train or improve AI models unless you explicitly opt in?
- [ ] **Derived/inferred data included:** Do restrictions also cover derived/inferred data (e.g., telemetry insights, embeddings, model artifacts)?
- [ ] **Encryption:** Does the contract require encryption at rest and in transit, and address protection during processing where applicable?

Incident survivability

- [ ] **Incident/outage notice timelines:** Are notice timelines defined in hours (not “promptly”)?
- [ ] **Log access:** Do you have contractual access to relevant logs for investigation (including during incidents)?
- [ ] **Vulnerability/patch disclosure:** Does the vendor commit to disclosing vulnerabilities and patch status relevant to your service?
- [ ] **Recovery commitments:** Are recovery objectives and responsibilities defined (e.g., RTO/RPO, restore processes, and support during outages/incidents)?

Third-party risk control

- [ ] **Sub processor disclosure:** Are subcontractors/sub processors disclosed (at least for material services)?
- [ ] **Flow-down obligations:** Are the vendor’s security/privacy obligations contractually flowed down to sub processors?

Commercial/legal terms that decide your exposure

- ☐ **Liability/indemnity fairness:** Do the liability and indemnity terms avoid shifting the vendor's security failures onto you?
- ☐ **Exit + deletion proof:** Are exit processes defined (export formats, timelines, costs) and is deletion verifiable (including backups/replicas)?

Figure 1. The 80/20 Priorities: CORE 12 visual from CSEC Recommended Cyber Security Contract (Datarisk Canada)

4.2 Stop/Go triggers and escalation

The following are treated as Stop/Go items for most SMEs. If any are missing or unacceptable, Datarisk Canada recommends executive sign-off and a documented mitigation plan, or selecting an alternate vendor.

- ☐ Vendor can use your data (or derived data) beyond service delivery, including AI training, without your explicit opt-in.
- ☐ Incident notification and investigation support are vague, delayed, or contingent on additional fees.
- ☐ Subprocessors are opaque and obligations do not flow down.
- ☐ Liability/indemnities create one-way exposure (you carry the vendor's risk), or remedies are effectively meaningless for security incidents.
- ☐ Exit is punitive or unclear (high lock-in risk), or deletion cannot be verified.

Figure 2. The 80/20 Priorities: Stop/Go Triggers and Escalation visual from CSEC Recommended Cyber Security Contract (Datarisk Canada)

5. Fast contract navigation

Vendor contract terms are often scattered across multiple documents. Use a fast scan approach (quickly surveying a broad range of IPs or ports with lightweight scanning tools and default settings) before deep review:

Search terms to find the relevant clauses quickly:

- [ ] **Data:** “Customer Data”, “Confidential Information”, “metadata”, “telemetry”, “derived”, “inferred”, “analytics”, “improve”
- [ ] **AI:** “machine learning”, “model”, “training”, “fine-tuning”, “embedding”, “LLM”
  Incidents: “Security Incident”, “breach”, “notification”, “cooperate”, “forensics”, “incident response”
- [ ] **Evidence:** “logs”, “audit logs”, “retention”, “monitoring”, “SIEM”
- [ ] **Third parties:** “subprocessor”, “subcontractor”, “affiliate”, “third party”
- [ ] **Liability:** “indemnify”, “indemnification”, “limitation of liability”, “liability cap”, “consequential”
- [ ] **Exit:** “termination”, “return of data”, “export”, “deletion”, “destroy”, “survival”
- [ ] **Residency:** “region”, “location”, “data residency”, “transfer”, “cross-border”

6. Practical playbook when terms are hard to negotiate

Many scaled SaaS vendors and hyperscalers have limited flexibility in their MSAs. This checklist supports a realistic approach: negotiate where feasible, and apply compensating controls where necessary.

If data use terms are broad (“we may use data to improve services”)

- [ ] Restrict data categories: avoid uploading sensitive data unless necessary.
- [ ] Disable optional training/telemetry features where available and document the configuration.
- [ ] Segment workloads so high-sensitivity systems use vendors with stronger commitments.
- [ ] Require written clarification of what “improve services” means and what is excluded.

If incident response language is vague (“promptly”, “as required by law”)

- [ ] Secure a SOW addendum with hours-based notice, log access, and cooperation obligations.
- [ ] Purchase the tier that includes logs and incident support if this is the only viable route.
- [ ] Require an escalation path and a named incident response contact process.

If liability is capped too low or remedies are "service credits only"

- [ ] Treat the service as unsuitable for high-sensitivity workloads.
- [ ] Reduce blast radius (limit integration depth, limit stored data).
- [ ] Document risk acceptance and ensure internal contingency planning is proportionate.

If subprocessors are opaque

- [ ] Require a published subprocessor list and change notifications.
- [ ] If not available, restrict use to low-risk data/workloads or select an alternative vendor

7. Documentation and evidence standards

For each checklist item, record:

- [ ] the document (MSA/DPA/SOW/Exhibit/Policy),
- [ ] the clause number and title (or URL + version/date),
- [ ] the exact limitation/commitment, and
- [ ] any conditions (e.g., "paid tier only", "upon request", "best efforts", "sole discretion").

A strong vendor assessment file allows your organization to:

- [ ] justify risk acceptance decisions,
- [ ] support audits and insurance applications, and
- [ ] respond faster during incidents.

8. Glossary

- [ ] **MSA:** Master Services Agreement or equivalent main contract framework.
- [ ] **SOW:** Statement of Work; typically where scope, SLAs, and operational commitments live.
- [ ] **DPA:** Data Processing Addendum; often governs personal information handling and subprocessors.
- [ ] **Security Exhibit:** Technical and security commitments (logging, encryption, IR, controls).
- [ ] **Policy:** Online terms incorporated by reference (acceptable use, security policy, subprocessor list).
- [ ] **Derived/Inferred Data:** Data created from your usage (analytics, telemetry insights, embeddings, model artifacts) that can still create confidentiality and privacy risk.

CSP Audit (Prioritized List)

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🔴	CORE 12	B3.1	Data use limitation: Does the contract prohibit the vendor from using our data except to deliver the service?						
🔴	CORE 12	J1.1	AI training restriction: Does the contract prohibit using our data to train/improve vendor AI/models unless we explicitly opt in?						
🔴	CORE 12	J1.2	Derived data AI restriction: Does the prohibition also cover derived/inferred data and telemetry-based learning?						
🔴	CORE 12	B1.1	Encryption: Does the contract require encryption at rest and in transit?						
🔴	CORE 12	F1.1	Notification timelines: Are incident/outage notification timelines defined (not just “promptly”)?						
🔴	CORE 12	F2.1	Log access: Will we get access to relevant logs needed for investigation?						
🟠	CORE 12	F2.2	Vulnerability/patch disclosure: Must the vendor disclose relevant vulnerabilities and patches?						
🟠	CORE 12	F3.1	Recovery targets: Are recovery targets defined (e.g., RTO/RPO or equivalent) and enforceable?						
🔴	CORE 12	D1.1	Subcontractor disclosure: Does the vendor disclose subcontractors/subprocessors and critical suppliers?						
🔴	CORE 12	D1.2	Flow-down: Do the vendor’s security/privacy obligations flow down to subcontractors?						
🔴	CORE 12	K2.1	Liability/indemnity clarity: Are liability and indemnification terms clear and do they avoid shifting the vendor’s security failures onto us?						
🟠	CORE 12	K4.1	Exit & deletion proof: Are exit steps defined (export support + verifiable deletion, including backups) with timelines/costs?						

CSP Audit (Prioritized List)

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🟡	Full Checklist	A1.1	Service model: Does the contract clearly state whether the service is IaaS / PaaS / SaaS (or MSSP/AI) and what that means for responsibility boundaries?						
🟡	Full Checklist	A1.2	Responsibility matrix: Is there a contractually binding “who does what” matrix (not just marketing material)?						
🟡	Full Checklist	A2.1	Accountability: Does the contract explicitly acknowledge that we remain accountable for our data even if the vendor hosts/processes it?						

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🔴	Full Checklist	B1.2	Processing protection: Does it address protection during processing (not only storage/transport)?						
🔴	Full Checklist	B2.1	Vendor staff access limits: Are vendor personnel access restrictions defined (need-to-know, RBAC, privileged controls)?						
🔴	Full Checklist	B2.2	Auditability: Are vendor access events logged and auditable?						
🔴	Full Checklist	B3.2	Derived/inferred data: Does it explicitly restrict vendor use of inferred/derived data (e.g., embeddings, telemetry insights, model artefacts) as well?						
🔴	Full Checklist	B4.1	Secure deletion: Are secure deletion obligations defined (including backups/replicas) and verifiable?						
🟠	Full Checklist	B4.2	Recovery: Are recovery processes defined (what is recoverable, timelines, and conditions)?						

CSP Audit (Prioritized List)

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🟠	Full Checklist	C1.1	Approved regions: Does the contract specify approved geographic regions where data will be stored/processed?						
🟠	Full Checklist	C1.2	All data types: Does residency apply to production data, logs, metadata, backups, and derived data (explicitly)?						
🟠	Full Checklist	C2.1	Data movement: Must the vendor notify and obtain approval before moving data outside approved regions?						
🟠	Full Checklist	C3.1	Verification: Does the vendor provide transparency/tooling to verify data location?						
🟠	Full Checklist	C4.1	Exit affordability: Are data exit/migration options affordable and practical (anti–lock-in)?						
🟠	Full Checklist	C4.2	Exit details: Are export formats, timelines, assistance, and costs defined?						

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🔴	Full Checklist	D2.1	Supply chain risk plan: Does the vendor maintain a supply chain risk management plan and support our assessments?						
🟠	Full Checklist	D2.2	Foreign ownership/sourcing: Does it address risks related to foreign ownership and hardware/firmware/software sourcing?						

CSP Audit (Prioritized List)

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🟠	Full Checklist	E1.1	MFA: Is multi-factor authentication required for relevant access?						
🟠	Full Checklist	E1.2	Least privilege: Are role-based and least-privilege controls required?						
🔴	Full Checklist	E2.1	Privileged access: Is privileged access management required and auditable?						
🟠	Full Checklist	E3.1	Federation controls: Are restrictions/conditions on identity federation defined?						
🟠	Full Checklist	E3.2	Backdoor/API controls: Are there controls to prevent backdoors or unauthorized API access?						

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🔴	Full Checklist	F1.2	Customer obligations support: Does the vendor commit to notifying us fast enough to meet our legal/regulatory obligations?						
🟠	Full Checklist	F3.2	IR coordination: Is incident coordination defined (roles, communications, handoffs)?						
🟠	Full Checklist	F3.3	24/7 monitoring (if critical): For regulated/critical services, is 24/7 monitoring and formal IR support required?						

CSP Audit (Prioritized List)

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
	Full Checklist	G1.1	Continuous monitoring: Does the contract require continuous threat/vulnerability monitoring?						
	Full Checklist	G1.2	Logging requirements: Are key security/access events logged with retention/access/format defined?						
	Full Checklist	G2.1	Scanning & pen testing: Are regular vulnerability scanning and penetration testing commitments included?						
	Full Checklist	G3.1	DoS resilience: Are protections against denial-of-service attacks included?						
	Full Checklist	G4.1	Reporting: Does the vendor report security posture/performance metrics on a defined schedule?						

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
	Full Checklist	H1.1	Patching timelines: Are timely patching obligations defined (ideally severity-based)?						
	Full Checklist	H2.1	Known issue disclosure: Must the vendor disclose known security issues affecting the service?						
	Full Checklist	H3.1	Open-source risk: Does the vendor manage open-source software risks (SBOM/SCA expectations if applicable)?						
	Full Checklist	H4.1	Security-impacting changes: Must the vendor provide advance notice of changes that affect security?						

CSP Audit (Prioritized List)

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🟡	Full Checklist	I1.1	Privacy risk management: Does the vendor support privacy risks being assessed and managed (as applicable)?						
🟡	Full Checklist	I2.1	Personnel screening: Are vendor staff appropriately screened for privileged roles?						
🟡	Full Checklist	I3.1	Physical security: Are physical access controls/monitoring for data centres addressed?						
🟡	Full Checklist	I4.1	Retention & destruction: Are retention and destruction obligations clearly defined and verifiable?						

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🟠	Full Checklist	J2.1	Cryptographic agility: Does the contract require cryptographic agility (ability to upgrade crypto as threats evolve)?						

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🟡	Full Checklist	K1.1	IP ownership clarity: Does the contract clearly state who owns our data, outputs, vendor tools, and any joint artefacts?						
🟡	Full Checklist	K1.2	Confidentiality/trade secrets: Are trade secret and confidentiality protections clearly defined?						
🔴	Full Checklist	K2.2	Customer indemnities: Do we avoid broad customer indemnities that make us responsible for vendor failures?						

CSP Audit (Prioritized List)

Priority	Group	Section	Question	Meets	Partial	No	N/A	Where to find it	Notes / Evidence (Clause reference, URL, page, screenshot)
🔴	Full Checklist	K2.3	Liability caps: Do caps/exclusions avoid gutting remedies for incidents, confidentiality breaches, and security failures?						
🟠	Full Checklist	K3.1	Support model/offshore access: If offshore access exists, is it restricted, approved, and auditable?						

Complete CSP Audit

Section	Question	Meets	Partial	No	N/A	Notes
A1.1	Service model: Does the contract clearly state whether the service is IaaS / PaaS / SaaS (or MSSP/AI) and what that means for responsibility boundaries?					
A1.2	Responsibility matrix: Is there a contractually binding “who does what” matrix (not just marketing material)?					
A2.1	Accountability: Does the contract explicitly acknowledge that we remain accountable for our data even if the vendor hosts/processes it?					

Section	Question	Meets	Partial	No	N/A	Notes
B1.1	Encryption: Does the contract require encryption at rest and in transit?					
B1.2	Processing protection: Does it address protection during processing (not only storage/transport)?					
B2.1	Vendor staff access limits: Are vendor personnel access restrictions defined (need-to-know, RBAC, privileged controls)?					
B2.2	Auditability: Are vendor access events logged and auditable?					
B3.1	Data use limitation: Does the contract prohibit the vendor from using our data except to deliver the service?					
B3.2	Derived/inferred data: Does it explicitly restrict vendor use of inferred/derived data (e.g., embeddings, telemetry insights, model artefacts) as well?					
B4.1	Secure deletion: Are secure deletion obligations defined (including backups/replicas) and verifiable?					
B4.2	Recovery: Are recovery processes defined (what is recoverable, timelines, and conditions)?					

Complete CSP Audit

Section	Question	Meets	Partial	No	N/A	Notes
C1.1	Approved regions: Does the contract specify approved geographic regions where data will be stored/processed?					
C1.2	All data types: Does residency apply to production data, logs, metadata, backups, and derived data (explicitly)?					
C2.1	Data movement: Must the vendor notify and obtain approval before moving data outside approved regions?					
C3.1	Verification: Does the vendor provide transparency/tooling to verify data location?					
C4.1	Exit affordability: Are data exit/migration options affordable and practical (anti–lock-in)?					
C4.2	Exit details: Are export formats, timelines, assistance, and costs defined?					

Section	Question	Meets	Partial	No	N/A	Notes
D1.1	Subcontractor disclosure: Does the vendor disclose subcontractors/subprocessors and critical suppliers?					
D1.2	Flow-down: Do the vendor's security/privacy obligations flow down to subcontractors?					
D2.1	Supply chain risk plan: Does the vendor maintain a supply chain risk management plan and support our assessments?					
D2.2	Foreign ownership/sourcing: Does it address risks related to foreign ownership and hardware/firmware/software sourcing?					

Section	Question	Meets	Partial	No	N/A	Notes
E1.1	MFA: Is multi-factor authentication required for relevant access?					
E1.2	Least privilege: Are role-based and least-privilege controls required?					

Complete CSP Audit

Section	Question	Meets	Partial	No	N/A	Notes
E2.1	Privileged access: Is privileged access management required and auditable?					
E3.1	Federation controls: Are restrictions/conditions on identity federation defined?					
E3.2	Backdoor/API controls: Are there controls to prevent backdoors or unauthorized API access?					

Section	Question	Meets	Partial	No	N/A	Notes
F1.1	Notification timelines: Are incident/outage notification timelines defined (not just “promptly”)?					
F1.2	Customer obligations support: Does the vendor commit to notifying us fast enough to meet our legal/regulatory obligations?					
F2.1	Log access: Will we get access to relevant logs needed for investigation?					
F2.2	Vulnerability/patch disclosure: Must the vendor disclose relevant vulnerabilities and patches?					
F3.1	Recovery targets: Are recovery targets defined (e.g., RTO/RPO or equivalent) and enforceable?					
F3.2	IR coordination: Is incident coordination defined (roles, communications, handoffs)?					
F3.3	24/7 monitoring (if critical): For regulated/critical services, is 24/7 monitoring and formal IR support required?					

Section	Question	Meets	Partial	No	N/A	Notes
G1.1	Continuous monitoring: Does the contract require continuous threat/vulnerability monitoring?					
G1.2	Logging requirements: Are key security/access events logged with retention/access/format defined?					

Complete CSP Audit

Section	Question	Meets	Partial	No	N/A	Notes
G2.1	Scanning & pen testing: Are regular vulnerability scanning and penetration testing commitments included?					
G3.1	DoS resilience: Are protections against denial-of-service attacks included?					
G4.1	Reporting: Does the vendor report security posture/performance metrics on a defined schedule?					

Section	Question	Meets	Partial	No	N/A	Notes
H1.1	Patching timelines: Are timely patching obligations defined (ideally severity-based)?					
H2.1	Known issue disclosure: Must the vendor disclose known security issues affecting the service?					
H3.1	Open-source risk: Does the vendor manage open-source software risks (SBOM/SCA expectations if applicable)?					
H4.1	Security-impacting changes: Must the vendor provide advance notice of changes that affect security?					

Section	Question	Meets	Partial	No	N/A	Notes
I1.1	Privacy risk management: Does the vendor support privacy risks being assessed and managed (as applicable)?					
I2.1	Personnel screening: Are vendor staff appropriately screened for privileged roles?					
I3.1	Physical security: Are physical access controls/monitoring for data centres addressed?					
I4.1	Retention & destruction: Are retention and destruction obligations clearly defined and verifiable?					

Complete CSP Audit

Section	Question	Meets	Partial	No	N/A	Notes
J1.1	AI training restriction: Does the contract prohibit using our data to train/improve vendor AI/models unless we explicitly opt in?					
J1.2	Derived data AI restriction: Does the prohibition also cover derived/inferred data and telemetry-based learning?					
J2.1	Cryptographic agility: Does the contract require cryptographic agility (ability to upgrade crypto as threats evolve)?					

Section	Question	Meets	Partial	No	N/A	Notes
K1.1	IP ownership clarity: Does the contract clearly state who owns our data, outputs, vendor tools, and any joint artefacts?					
K1.2	Confidentiality/trade secrets: Are trade secret and confidentiality protections clearly defined?					
K2.1	Liability/indemnity clarity: Are liability and indemnification terms clear and understood (no hidden risk transfer)?					
K2.2	Customer indemnities: Do we avoid broad customer indemnities that make us responsible for vendor failures?					
K2.3	Liability caps: Do caps/exclusions avoid gutting remedies for incidents, confidentiality breaches, and security failures?					
K3.1	Support model/offshore access: If offshore access exists, is it restricted, approved, and auditable?					
K4.1	Exit & deletion proof: Are exit steps defined (export support + deletion proof, including backups) with timelines/costs?					