SSB DEFENCE

NIS2 READINESS GUIDE

Cybersecurity, Supply Chains and European Requirements for Canadian Organizations

Canadian exporters & suppliers • Manufacturers
Food production & supply chain • Organizations operating in the EU

PRACTICAL GUIDANCE FOR BUSINESS LEADERS

Version 1.0 | August 2026

Important notice

This guide provides general cybersecurity and business-readiness information. It is not legal advice and does not determine whether a particular organization is subject to NIS2 or a Member State's implementing law. Organizations should obtain jurisdiction-specific legal advice where required.

Executive Summary

NIS2 changes the way cybersecurity is treated across the European Union. For organizations in scope, cybersecurity is no longer simply an IT matter: it is a management, operational resilience, supply-chain and governance responsibility.

Canadian organizations should pay attention even when they are not directly regulated. A Canadian manufacturer, food producer, technology provider or other supplier may be asked by an EU customer to demonstrate security controls because NIS2 requires covered entities to address cybersecurity risks in their supplier relationships.

The practical question

Do not begin with “Are we compliant?” Begin with: “What services, systems, suppliers and business processes would matter most if they were disrupted - and can we demonstrate that we manage those risks?”

What this guide will help you do

- Understand NIS2 in plain business language.
- Recognize when a Canadian organization may face direct or indirect NIS2-related requirements.
- Understand the 10 core cybersecurity risk-management areas.
- Identify supply-chain and food-sector considerations.
- Prepare management, incident-response and business-continuity processes.
- Build a practical readiness roadmap without replacing technology simply because it is old.

A 2026 Poland note

Poland's amended Act on the National Cybersecurity System (KSC), implementing NIS2, entered into force on 3 April 2026. Polish guidance states that entities meeting the criteria on that date generally have until 3 October 2026 to register in the KSC list, until 3 April 2027 to implement the new obligations, and certain essential entities have until 3 April 2028 for their first mandatory cybersecurity audit.

For organizations in Poland

Self-identification matters. Polish authorities advise organizations to examine their actual activities, sector, size and applicable KSC provisions rather than relying only on a business classification code.

1. NIS2 in Plain Language

Directive (EU) 2022/2555 - commonly called NIS2 - establishes a higher common level of cybersecurity across the EU. It expands the range of sectors covered, strengthens risk-management and incident-reporting requirements, and places greater emphasis on management oversight and supply-chain security.

Who is generally in scope?

At EU level, NIS2 generally applies to public or private entities of a type listed in Annex I or Annex II that qualify as medium-sized enterprises or exceed the medium-enterprise thresholds and provide services or carry out activities within the Union. There are important exceptions and special rules, so size alone does not decide scope.

Examples of covered sectors

Higher criticality sectors	Other critical sectors
Energy • Transport • Banking • Financial market infrastructure • Health • Drinking water • Waste water • Digital infrastructure • ICT service management • Public administration • Space	Postal/courier • Waste management • Chemicals • Food • Certain manufacturing • Digital providers • Research

Essential vs. important entities

NIS2 distinguishes between essential and important entities. Both categories are subject to cybersecurity risk-management and reporting duties; the supervisory and enforcement approach differs. National implementing law determines how these categories operate in practice.

Canadian organizations

A company located only in Canada is not automatically subject to NIS2 merely because it sells into Europe. Direct applicability depends on the Directive, the relevant national law, the organization's activities and establishment/service circumstances. Indirect contractual and supply-chain requirements can still be significant.

2. Canadian Business & European Supply Chains

NIS2 explicitly requires covered entities to address supply-chain security, including security aspects of relationships with direct suppliers and service providers. This is why NIS2 can matter commercially to a Canadian organization even where the Canadian organization is not itself a regulated NIS2 entity.

What an EU customer may ask from a supplier

- Evidence of cybersecurity policies and risk assessments.
- Multi-factor authentication and access-control practices.
- Incident-notification obligations and defined escalation contacts.
- Vulnerability and patch-management processes.
- Backup, recovery and business-continuity capabilities.
- Security requirements for subcontractors and service providers.
- Asset inventories and ownership of critical systems.
- Cybersecurity training and basic cyber-hygiene controls.
- Contractual rights to request evidence, audits or remediation.

Treat customer requirements as operational requirements

A questionnaire from a European customer should not become a paper exercise. If a supplier says it has controls, it should be able to demonstrate that those controls exist and are maintained. Evidence may include policies, system records, training records, risk registers, recovery-test results, supplier reviews and management approvals.

SSB Defence perspective

Compliance documentation should describe the business as it actually operates. A simple control that works consistently is stronger than a complex policy that exists only on paper.

3. Food Production & the European Food Supply Chain

Food is specifically included among NIS2's other critical sectors. Annex II covers food businesses engaged in wholesale distribution and industrial production and processing. National implementing laws determine the detailed application in each Member State.

This is particularly relevant in Poland and other EU countries with significant food production, processing, storage and distribution operations. Cybersecurity failures can affect more than office systems: they can interrupt production, traceability, refrigeration, warehousing, logistics and the ability to move product.

PRODUCER	PROCESSOR	STORAGE	LOGISTICS	WHOLESALE

Systems that deserve special attention

- Production-control and industrial systems that affect processing or packaging.
- Refrigeration, environmental and cold-chain monitoring.
- Warehouse, inventory and traceability systems.
- ERP, purchasing, scheduling and order-management systems.
- Quality-control and laboratory systems.
- Remote vendor access to production equipment.
- Transportation and logistics platforms.
- Backups and recovery processes for production-critical data.

Operational reality

A food plant may have equipment that remains productive for decades while the computer or operating system controlling it becomes obsolete. The goal is not to replace functioning equipment blindly; it is to understand the dependency, reduce exposure and plan for failure or transition.

4. The 10 Core NIS2 Risk-Management Areas

1 **Risk analysis & system security**
Maintain policies and a repeatable process for identifying, evaluating, prioritizing and treating cybersecurity risk.

2 **Incident handling**
Define how incidents are detected, escalated, contained, investigated, communicated and recovered from.

3 **Business continuity & crisis management**
Plan backups, disaster recovery, continuity of critical operations and decision-making during disruption.

4 **Supply-chain security**
Assess risks created by direct suppliers and service providers and establish proportionate contractual/security expectations.

5 **Secure acquisition, development & maintenance**
Address security when systems are purchased, built, changed and maintained, including vulnerability handling and disclosure.

6 **Effectiveness assessment**
Test whether controls actually work through reviews, exercises, technical validation and measurable evidence.

7 **Cyber hygiene & training**
Establish practical baseline practices and recurring training appropriate to roles and risks.

8 **Cryptography & encryption**
Use appropriate policies and controls to protect sensitive data and communications.

9 **HR security, access control & asset management**
Know what assets exist, who owns them, who can access them and how access changes when roles change.

10 **MFA & secure communications**
Use multi-factor or continuous authentication and secure communications where appropriate.

Proportionality matters

NIS2 requires appropriate and proportionate technical, operational and organizational measures. Risk exposure, organization size, likelihood and severity of incidents, societal/economic impact, state of the art and implementation cost all matter.

5. Management Responsibility

NIS2 makes cybersecurity a governance issue. At EU Directive level, management bodies of essential and important entities must approve cybersecurity risk-management measures and oversee their implementation. Management members are also required to receive training under the national implementation of NIS2.

Questions management should be able to answer

- Which business services would cause the greatest operational or financial harm if unavailable?
- Which systems, vendors and people do those services depend on?
- What risks have we formally accepted, and who approved that decision?
- Can we restore critical systems from backups, and when was recovery last tested?
- Who has authority during a cybersecurity incident?
- How quickly can we determine whether an incident is significant and reportable?
- Which suppliers have privileged or remote access to our environment?
- Where are our unsupported or difficult-to-replace systems?
- What evidence can we show a customer, auditor or regulator that our controls work?

Cybersecurity is not an IT-only delegation

IT may operate many controls, but business leadership owns decisions about risk tolerance, investment, continuity priorities and the consequences of disruption.

6. Incident Reporting - Prepare Before the Incident

At Directive level, significant incidents follow a staged reporting model: an early warning within 24 hours of awareness, an incident notification within 72 hours, and a final report generally within one month after the incident notification. National processes and sector-specific rules must also be checked.

24 HOURS	72 HOURS	1 MONTH
Early warning	Incident notification	Final report / progress where applicable

7. Legacy & Operational Technology

Operational organizations frequently depend on technology that cannot follow a normal three-to-five-year IT replacement cycle. Production machinery, building controls, laboratory equipment, point-of-sale systems, property-management systems and proprietary applications may remain essential long after the supporting operating system or hardware becomes difficult to maintain.

Legacy does not automatically mean insecure

The risk comes from unmanaged exposure. A legacy system can often be operated more safely when its role, dependencies and limitations are understood and proportionate compensating controls are applied.

IDENTIFY	ISOLATE	PROTECT	RECOVER	TRANSITION
Document the system, business purpose, owner, interfaces, remote access, software dependencies and failure impact.	Segment networks, restrict unnecessary connectivity, limit internet access and tightly control administrative paths.	Use least privilege, MFA where feasible, monitored access, backups, allow-listing or other compensating controls.	Know how the system, configuration and production data will be restored if hardware or software fails.	Build a realistic modernization plan around operational windows, vendor constraints, cost and business continuity.

Business before technology

Replacing an operational system can create its own risk. The correct decision may be to secure and isolate an existing system while developing a controlled migration plan.

8. NIS2 Readiness Checklist

Use this as a management-level starting point. A checked box should mean the organization can demonstrate the control, not simply that a policy mentions it.

☐ Scope: We have assessed whether our activities fall within NIS2 or relevant national implementing legislation.

☐ Customers: We know which EU customers or contracts impose cybersecurity requirements on us.

☐ Ownership: Critical services and systems have named business and technical owners.

☐ Assets: We maintain an inventory of critical hardware, software, cloud services and operational technology.

☐ Risk: Cybersecurity risks are documented, prioritized and reviewed.

☐ Access: Privileged access is limited, reviewed and protected with MFA where appropriate.

☐ Joiners/movers/leavers: Access changes when personnel roles change or employment ends.

☐ Vulnerabilities: We have a process for patching, mitigation and handling systems that cannot be patched.

☐ Backups: Critical data and configurations are backed up and protected from routine administrative access.

☐ Recovery: We have tested restoration of critical systems.

☐ Continuity: The business has defined how critical operations continue during technology outages.

☐ Incident response: Roles, escalation paths, evidence preservation and communications are documented.

☐ Reporting: We can rapidly determine whether an incident may trigger customer, contractual or regulatory reporting.

☐ Suppliers: Critical suppliers and service providers are identified and risk-ranked.

☐ Remote access: Third-party remote access is controlled, time-limited where practical and logged.

☐ Training: Management and staff receive role-appropriate cybersecurity training.

☐ Encryption: Sensitive information and communications are protected appropriately.

☐ Monitoring: Security-relevant events are logged and reviewed at a level proportionate to risk.

☐ Testing: We periodically test whether controls work rather than relying only on documentation.

☐ Management: Leadership reviews cybersecurity risk, priorities, exceptions and investment decisions.

9. Building a Practical Roadmap

Readiness is more effective when treated as a business-improvement program rather than a one-time compliance project. SSB Defence uses a five-stage approach that keeps operational needs and risk priorities at the centre.

01 DISCOVER

Understand the business, critical services, technology, people, suppliers and regulatory/customer context.

02 ASSESS

Evaluate cybersecurity, resilience, legacy dependencies, evidence and gaps against applicable requirements.

03 PLAN

Prioritize actions according to business impact, risk, cost, operational constraints and realistic timelines.

04 PROTECT

Implement or coordinate practical controls, documentation, training, recovery capabilities and supplier measures.

05 EVOLVE

Reassess as the organization, threats, technology, customers and regulatory requirements change.

Prioritize by consequence

Not every finding needs the same urgency. A practical roadmap considers what could stop production, harm customers, create regulatory exposure, prevent recovery, compromise sensitive information or create a dangerous dependency on a single person, vendor or unsupported system.

Sometimes the best technology decision is deciding not to add more technology.

Complexity has a security and operating cost. Preserve effective business practices, improve what matters and add technology where it creates a measurable benefit.

10. Poland - 2026 Implementation Snapshot

For organizations operating in Poland, the 2026 amendment to the Act on the National Cybersecurity System (KSC) is now in force. It implements NIS2 through Polish national law and creates specific Polish registration, implementation, incident-management and audit obligations.

Date	Milestone
3 April 2026	KSC amendment entered into force.
7 May - 3 October 2026	Self-registration period for entities not entered ex officio, according to Polish government guidance.
3 October 2026	Registration deadline for entities meeting the criteria when the amendment entered into force.
3 April 2027	Deadline identified by Polish guidance for implementing the new obligations for entities meeting the criteria on entry into force; connection to S46 also required.
3 April 2028	First mandatory cybersecurity audit deadline for certain essential entities; subsequent audits at least every three years.

Polish self-identification

Poland's Ministry of Digital Affairs advises organizations to review their actual activity, applicable sector/subsector, size and the criteria in the KSC Act. PKD codes can assist, but the actual nature of the activity is decisive.

Food in Poland

Polish implementation materials explicitly identify production and distribution of food among the newly expanded sectors. Food businesses should assess their precise activity and size against the Polish KSC rules rather than assuming that all agricultural or food businesses are automatically covered.

How SSB Defence Can Help

NIS2 readiness should produce a stronger, more resilient business - not simply a larger collection of policies. SSB Defence helps organizations understand their environment, identify meaningful risk and build practical improvements around real operations.

A sensible starting point

- NIS2 / KSC scope and readiness discussion.
- Business technology risk assessment.
- Critical-system and legacy-technology review.
- Supply-chain and third-party risk review.
- Business continuity and recovery assessment.
- Cybersecurity policy and evidence-gap review.
- Prioritized remediation roadmap.

Start with a conversation

If your organization supplies European customers, operates in Poland or another EU Member State, or is being asked to demonstrate NIS2-related cybersecurity controls, begin by understanding the requirement and the business context before purchasing technology.

Sources & Further Reading

European Union - Directive (EU) 2022/2555 (NIS2)
https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Commission - NIS2 Directive FAQs
https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

ENISA - NIS2 Technical Implementation Guidance (26 June 2025)
https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

Poland - Ministry of Digital Affairs: KSC amendment overview (14 April 2026)
https://www.gov.pl/web/baza-wiedzy/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa

Poland - Ministry of Digital Affairs: KSC obligations (5 June 2026)
https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---obowiazki-podmiotow-kluczowych-i-waznych

Poland - Ministry of Digital Affairs: Self-identification guidance (27 April 2026)
https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---jak-dokonac-samoidentyfikacji

Poland - Act of 23 January 2026 amending the National Cybersecurity System Act
https://eli.gov.pl/eli/DU/2026/252/ogl

SSB DEFENCE

Business First. Technology Second.