Bulletin | Cybersecurity, Privacy and Data Protection

October 2023

NIST Cybersecurity Framework 2.0 – A Canadian Perspective

In August 2023, the U.S. National Institute of Standards and Technology released a public draft of an updated *Cybersecurity Framework* with significant changes, including an emphasis on governance and supply chain risk management that align with Canadian legal requirements and regulatory guidance. The updated Framework will be an important benchmark resource for Canadian organizations of all kinds and sizes.

Background

The National Institute of Standards and Technology (NIST) is a U.S. Department of Commerce agency whose mission is to promote American innovation and industrial competitiveness. The NIST *Cybersecurity Framework* (the "CSF") provides guidance for managing cybersecurity risks by helping organizations understand, assess, prioritize, and communicate about those risks and the actions that will reduce them. The first version of the CSF, designed for use by critical infrastructure operators, was published in 2014. The current version, *CSF 1.1*, was published in 2018. In addition, in 2016, NIST published simplified cybersecurity guidance titled *Small Business Information Security: The Fundamentals* based on the CSF. See BLG bulletin *Cybersecurity Guidance for Small and Medium Size Enterprises*.

The CSF, particularly its "Framework Core", has been endorsed as a foundational cybersecurity resource by regulators and industry associations around the world, including in Canada. For example, the CSF Framework Core is reflected in the Investment Industry Regulatory Organization of Canada's *Cybersecurity Best Practices Guide* and *Cyber Security Self Assessment*, the BC Financial Services Authority's *Information Security Guideline*, the Mutual Fund Dealers Association of Canada's *Cybersecurity bulletin*, the Ontario Energy Board's *Ontario Cyber Security Framework*, and the Chartered Professional Accountants Canada's *20 questions directors should ask about cybersecurity*.

Cybersecurity Framework 2.0

General

In August 2023, NIST announced a public draft of an updated *Cybersecurity Framework 2.0* (CSF 2.0), a Discussion Draft of Implementation Examples, and a CSF 2.0 Reference Tool. NIST is accepting public comment on draft CSF 2.0 until November 2023, and plans to publish the final version of CSF 2.0 in early 2024.

NIST explained that draft CSF 2.0 reflects changes in the cybersecurity landscape and makes it easier for organizations in all sectors to implement the CSF. The significant changes include:

- A new title ("Cybersecurity Framework" instead of "Framework for Improving Critical Infrastructure Cybersecurity") and an expanded scope (providing cybersecurity guidance for "any organization – regardless of its size, sector, or maturity" instead of critical infrastructure).
- A modified Framework Core (which describes the main "functions" or "primary pillars" of a successful and holistic cybersecurity program) with a new Govern function in addition to the previous functions – Identify, Protect, Detect, Respond, and Recover.
- Improved and expanded implementation guidance, including examples and templates.
- Additional guidance for integrating cyber risk management with privacy risk management (including the use of NIST's *Privacy Framework*) and enterprise risk management.

New Govern Function

The new Govern function in draft CSF 2.0 Framework Core is a significant change. The function requires an organization to "[e]stablish and monitor the organization's cybersecurity risk management strategy, expectations, and policy", and "directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy".

Draft CSF 2.0 considers the Govern function to be cross-cutting because it informs how an organization will achieve and prioritize the outcomes of the other five functions of the Framework Core in the context of the organization's mission and stakeholder expectations.

Image source: NIST

The Govern function has the following six high-level "categories" (i.e., outcomes), each of which has numerous "sub-categories" (i.e., sub-outcomes):

- **Organizational Context**: The circumstances – mission, stakeholder expectations, and legal, regulatory, and contractual requirements – surrounding the organization's cybersecurity risk management decisions are understood.
- **Risk Management Strategy**: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.
- **Cybersecurity Supply Chain Risk Management**: Cybersecurity supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.
- **Roles, Responsibilities, and Authorities**: Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.
- **Policies, Processes, and Procedures**: Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced.
- **Oversight**: Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.

Supply Chain Risk Management

Draft CSF 2.0 explains that cybersecurity supply chain risk management is critical for organizations, and encourages the use of CSF 2.0 "to foster an organization's oversight and communications related to cybersecurity risks with stakeholders across supply chains". Draft CSF 2.0 addresses cybersecurity supply chain risk management in the "Cybersecurity Supply Chain Risk Management" category of the new Govern function by specifying the following desired outcomes:

- A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.
- Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.
- Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.
- Suppliers are known and prioritized by criticality.
- Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other agreements.
- Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.
- The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored throughout the relationship.
- Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.
- Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.
- Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.

Draft CSF 2.0 also encourages the use of NIST's *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161)* to help manage supply chain cybersecurity risk.

Comment

CSF 2.0 will be an important cybersecurity benchmark resource that aligns with Canadian legal requirements and regulatory guidance regarding cybersecurity governance and cybersecurity supply chain risk management.

Cybersecurity Governance

The new Govern function in draft CSF 2.0 aligns with Canadian regulatory guidance that emphasizes the importance of a governance framework for effective cyber risk management. For example, the Office of the Superintendent of Financial Institutions' *Guideline B-13 – Technology and Cyber Risk Management* and *Cyber Security Self Assessment*, the Investment Industry Regulatory Organization of Canada's *Cybersecurity Best Practices Guide*, and the BC Financial Services Authority's *Information Security Guideline*.

The new Govern function also aligns with Canadian privacy commissioner guidance (e.g., *Getting Accountability Right with a Privacy Management Program*) and governance requirements imposed by recent amendments to Québec's private sector privacy law and the federal government's proposed new *Consumer Privacy Protection Act*. See BLG bulletins *Québec Privacy Law Reform: Compliance Guide for Organizations* and *Canada's Consumer Privacy Protection Act (Bill C-27): Impact for businesses*.

Cybersecurity Supply Chain Risk

Draft CSF 2.0's increased emphasis on cybersecurity supply chain risk management aligns with Canadian regulatory guidance that emphasizes the importance of managing cybersecurity risks arising from relationships with suppliers and service providers. For example, the Office of the Superintendent of Financial Institutions' *Guideline B-10 – Third-Party Risk Management*, the Investment Industry Regulatory Organization of Canada's *Outsourcing Arrangements* and *Cyber Security Self Assessment*, the BC Financial Services Authority's *Outsourcing Guideline*, and the Canadian Centre for Cyber Security's *Cyber supply chain: An approach to assessing risk* and *Supply chain security for small and medium-sized organizations*.

Draft CSF 2.0's emphasis on cybersecurity supply chain risk management also aligns with Canadian privacy commissioner guidance for organizations who engage service providers to process/store personal information (e.g., *Privacy and outsourcing for businesses*). See BLG bulletin *Privacy Commissioner reports provide guidance for outsourcing agreements*.

For those reasons, Canadian organizations of all kinds and sizes should consider using CSF 2.0 as a foundational resource for assessing and improving their cybersecurity risk management program. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience in cyber risk management and crisis management legal services. Find out more at **blg.com/cybersecurity**.