Bulletin | Cybersecurity, Privacy and Data Protection

January 2022

BCFSA finalizes information security and outsourcing guidelines

In October 2021, the BC Financial Services Authority issued information security and outsourcing guidelines for provincially regulated financial institutions and pension plan administrators in British Columbia. Regulated entities should regularly review their outsourced services contracts and their information security and outsourcing policies, practices and procedures to ensure compliance with the guidelines and other legal requirements.

Information security and outsourcing risks

Information security risks are risks of losses and liabilities suffered or incurred by an organization resulting from a failure or breach of the systems used by or on behalf of the organization or its business partners, including incidents that affect the confidentiality, integrity or availability of data in the organization's possession or control. Information security risks can result from internal sources (e.g., employees, contract workers and system failures) or external sources (e.g., hackers, fraudsters and acts of nature). Information security risks are particularly relevant to financial institutions because information technology and data (both sensitive and legally regulated) are fundamental to their daily business operations.

Outsourcing risks are risks of losses and liabilities suffered or incurred by an organization resulting from a failure by an outsourced service provider to perform services for the organization in accordance with contractual requirements and applicable law. While outsourcing can provide significant benefits to the outsourcing organization, it can also present substantial risks arising from the organization's dependence on the outsourced service provider.

Canadian financial industry regulators and self-regulatory organizations have emphasized the importance of managing information security and outsourcing risks and have issued related guidance for regulated entities.

BCFSA guidelines

The BC Financial Services Authority ("BCFSA") is the provincial government regulator for financial institutions (i.e., credit unions, insurance companies and trust companies), pension plans and mortgage brokers in British Columbia, and is responsible for enforcing applicable legislation (e.g., *Financial Institutions Act* and *Pension Benefits Standards Act*). In 2021, BCFSA engaged in a consultation process regarding new information security and outsourcing guidelines for provincially regulated financial institutions and pension plan administrators (collectively "PRFIs"). BCFSA explained that information security and outsourcing are key risks for PRFIs and their stakeholders. BCFSA finalized and issued the guidelines in October 2021.

Information Security Guideline

The *Information Security Guideline* follows the National Institute of Standards and Technology *Cybersecurity Framework*, and includes incident reporting obligations similar to those set out in OSFI's *Advisory: Technology and Cyber Security Incident Reporting*. Following is a summary of key aspects of the guideline.

- **Scope:** The guideline applies broadly to all kinds of information and data (i.e., both personal information and business data in all formats) and all information systems (e.g., people, machines, methods of organization, and procedures) that handle or control functions relating to information and data.
- **Principles/expectations:** The guideline establishes high-level principles and specific procedures and practices that PRFIs are expected to implement and follow to mitigate information security ("IS") risks. The guideline should be implemented and applied in a risk-based and proportionate manner that considers differences in the nature, scope, complexity, systemic importance and risk profile of each PRFI.
- **Governance:** A PRFI's governing body (e.g., board of directors or plan administrator) is ultimately responsible for overseeing the prudent management of IS risks. A PRFI's governing body and senior management are expected to establish and implement policies and practices (including oversight activities), and allocate sufficient resources, to effectively and appropriately manage IS risks.
- **Risk management program:** A PRFI is expected to establish and document an effective IS risk management program (including specified policies, procedures and plans and internal compliance controls) that is integrated into the PRFI's overall risk management processes and is approved by the PRFI's governing body and reviewed at least once a year.
- **Identify:** A PRFI is expected to identify and assess IS risks to internal and external systems, people, assets, data and capabilities that enable the PRFI to achieve business objectives. The guideline specifies risk assessment and identification measures that PRFIs should implement.
- **Protect:** A PRFI is expected to protect its data and information systems in a reasonable and appropriate manner based on the sensitivity, value and criticality of the data and information systems. The guideline specifies security measures that PRFIs should implement.
- **Detect:** A PRFI is expected to establish monitoring processes to rapidly detect IS incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits and reporting. The guideline specifies detection measures that PRFIs should implement.
- **Respond:** A PRFI is expected to plan/develop and implement appropriate actions in response to IS incidents. The guideline specifies incident response procedures and practices that PRFIs should establish and execute.
- **Recover:** A PRFI is expected to plan/develop and implement appropriate activities for resilience and to restore capabilities/services and comply with applicable laws. The guideline specifies recovery plans, policies and practices that PRFIs should establish, test and execute.
- **Communication with BCFSA:** A PRFI is expected to inform the BCFSA of a "material" IS incident as soon as possible, and provide the BCFSA with an initial incident report within 72 hours and subsequent update reports throughout the incident response process. The guideline specifies criteria for determining whether an IS incident is "material" (based on the severity of the impact the incident will have on the PRFI's members, users, consumers and the public) and provides a template for reporting IS incidents to the BCFSA.
- **Outsourcing:** A PRFI that outsources information management services is expected to ensure that the outsourced service providers comply with applicable laws and the guideline in their treatment of the PRFI's information.

Outsourcing Guideline

The *Outsourcing Guideline* is based on OSFI's *Guideline B-10: Outsourcing of Business Activities, Functions and Processes*. Following is a summary of key aspects of the guideline.

- **Scope:** The guideline applies to all PRFIs (regardless of size) and to every outsourcing arrangement, which the guideline defines as "an agreement between a PRFI and a service provider whereby the service provider performs an activity, function or process that is, or could be, undertaken by the PRFI". The guideline explains that BCFSA will focus on outsourcing arrangements that are "material or support significant activities of the PRFI", and BCFSA will use "the principle of proportionality" to adjust its supervisory intensity depending on the "nature, size, complexity, and risk profile of the PRFI and the potential system impact of the PRFI's failure".
- **Principles/expectations:** The guideline establishes high-level principles to be proportionately implemented by all PRFIs and specific procedures and practices that PRFIs are expected to implement and follow to mitigate outsourcing risks. The guideline confirms that a PRFI remains accountable for all activities it outsources.
- **Governance and accountability:** A PRFI's governing body (e.g., board of directors or plan administrator) is ultimately responsible for all outsourced activities and is expected to support the monitoring, control and management of outsourcing risks through a sound governance structure. A PRFI's governing body and senior management are expected to establish and implement specific policies, practices and procedures (including oversight activities) for managing outsourcing risks.
- **Materiality:** A PRFI is expected to develop and implement a process for determining the materiality of each new and significantly changed outsourcing arrangement. All material outsourcing arrangements should be subject to an outsourcing risk management framework. The guideline specifies relaxed rules for intra-group outsourcing arrangements, and requirements and prohibitions regarding outsourcing arrangements with the PRFI's external auditor.
- **Risk management framework:** A PRFI is expected to ensure its enterprise risk management program appropriately manages and monitors risks commensurate with the materiality of its outsourcing arrangements, with particular attention to business continuity. The guideline specifies requirements for business continuity, monitoring and reporting, and location of records.
- **Risk assessments:** A PRFI is expected to identify outsourcing risks on an ongoing basis, promptly assess vulnerabilities in material outsourcing arrangements, and manage the resulting risks in accordance with the PRFI's risk tolerance and the guideline. The guideline specifies requirements for the assessments.
- **Due diligence:** A PRFI is expected to conduct initial and ongoing due diligence regarding an outsourcing arrangement to identify and assess risks associated with the arrangement and the service provider, including risks relating to subcontracted outsourced services.
- **Outsourcing contracts:** A PRFI is expected to document outsourcing arrangements with written contracts that address all elements of the arrangement and are reviewed by the PRFI's legal counsel. A PRFI is expected to ensure that each outsourcing contract addresses all issues relevant to managing the risks associated with the outsourcing arrangement to the extent feasible and reasonable, given the circumstances and having regard to the interests of the PRFI and its stakeholders. The guideline lists the following items to be addressed in contracts for material outsourcing arrangements: (1) nature and scope of services; (2) performance measures; (3) reporting requirements; (4) dispute resolution; (5) defaults and termination; (6) ownership and access; (7) contingency planning; (8) audit rights; (9) subcontracting; (10) pricing; (11) insurance; and (12) confidentiality, security and separation of property. A PRFI is expected to have formal processes for engaging and terminating service providers.
- **Information security:** A PRFI is expected to ensure its outsourcing service providers comply with all applicable laws (including personal information protection laws) and BCFSA's *Information Security Guideline* in the handling of the PRFI's data, records and items.

Recommendations for Compliance

PRFIs should review their information security and outsourcing policies, practices and procedures, and their current outsourced services contracts, on a regular basis to ensure compliance with BCFSA's information security and outsourcing guidelines. Following are some comments and suggestions.

- **Defensible decisions:** The guidelines contemplate they will be implemented and applied by each PRFI in a risk-based and proportionate manner suitable for the PRFI's particular circumstances and risk profile. That approach requires each PRFI's governing body and senior management to make risk-based business decisions consistent with the PRFI's risk tolerance. For those decisions to be reasonable and defensible, they should be informed (i.e., based on timely, complete and reliable information) and made honestly and in good faith with the benefit of appropriate advice from independent and qualified business, legal and technical experts. See BLG bulletin *Cyber risk management guidance for Canadian corporate directors*.
- **Other legal requirements:** In addition to compliance with the guidelines, PRFIs should be mindful of restrictions and requirements imposed by other applicable laws, including privacy/personal information protection laws, labour/employment laws, and securities laws applicable to reporting issuers (i.e., public companies). See BLG bulletins *Cyber Risk Management – Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*, *Frequently Asked Questions – Compliance with PIPEDA's Security Breach Obligations*, *Privacy Commissioner reports provide guidance for outsourcing agreements*.
- **Additional guidance:** A PRFI's implementation of the guidelines might benefit from consideration of guidance and best practices recommended by Canadian government agencies, regulators, privacy commissioners, industry associations and other organizations. See BLG bulletins *Cyber risk management guidance for Canadian corporate directors*, *Cybersecurity Technical Advisory from Five Eyes Cybersecurity Agencies*, *Cloud services – Guidance for managing cybersecurity risks*, *Financial Industry Regulator Issues Cybersecurity Guidance*, *Managing Insider Risk – Recent Best Practices Guidance*, *Cybersecurity Guidance for Small and Medium Organizations*, *Investment Funds Institute of Canada Issues Cybersecurity Guide*.
- **Legal privilege:** Risk management activities can result in sensitive communications and documents that might be subject to mandatory disclosure in regulatory investigations and litigation unless the communications and documents are protected by legal privilege. Consequently, PRFIs should take steps to establish and maintain legal privilege, where appropriate, over communications and documents relating to compliance with the guidelines and to help avoid inadvertent and unnecessary disclosures of legal advice. See BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*, *Cyber Risk Management – Legal Privilege Strategy (Part 2)*.
- **Insurance:** PRFIs should consider whether they have appropriate insurance for losses and liabilities resulting from information security and outsourcing incidents and for claims against directors and officers arising from the performance of their risk management duties and obligations. See BLG bulletin *Insurance for Cybersecurity Incidents and Privacy Breaches*. ■

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**.

BLG's Information Technology Group provides innovative, targeted legal services for IT operations including procurement processes, outsourcing agreements and disputes resolution. Find out more at **blg.com/informationtechnology**.