Bulletin | Cybersecurity, Privacy and Data Protection

August 2020

Cloud services – Guidance for managing cybersecurity risks

The Canadian Centre for Cyber Security has issued guidance for managing cybersecurity risks associated with cloud services. The guidance recognizes the significant benefits of cloud services, but cautions organizations to carefully assess and effectively manage the risks presented by cloud services. All organizations contemplating the use of cloud services can benefit from the Cyber Centre's guidance.

Cloud services

Cloud services make information technology ("IT") resources (e.g., networks, servers, software applications and data storage) and related services (e.g., hardware and software maintenance and technical support) available as a utility or consumption-based service. Cloud services enable an organization to outsource its IT requirements to a specialist cloud service provider (a "CSP") who can provide required services in a better and more efficient and cost-effective manner. For those reasons, cloud services can provide significant benefits, but they can also present potentially significant risks.

An organization that uses cloud services to operate its business or provide products or services to its customers remains responsible and liable for legal compliance and performance of the organization's legal obligations to investors, employees, customers and business partners. In addition, the organization is often dependent on the CSP and vulnerable to CSP misconduct, because the CSP usually has complete control over the quality and availability of the cloud service and physical custody of the organization's business data, including the organization's own sensitive/confidential data and third party data that is protected by restrictions/requirements imposed by contract, common/civil law or statute.

Those circumstances can present potentially significant risks to the organization, including risks relating to: (1) business continuity (if there are problems with the service or the CSP suspends or terminates the service); (2) data availability, integrity and confidentiality; and (3) legal compliance. Failure to manage those risks can result in various kinds of potentially significant claims and liabilities (e.g., lawsuits by shareholders, customers, employees and business partners, and investigations and enforcement proceedings by regulators) and losses (e.g., business disruption losses and reputational harm).

Legal framework

Canadian organizations use cloud services within a legal framework comprised of generally applicable laws (e.g., personal information protection laws, corporate directors' and officers' duties of care owed to their corporation, and common law and civil law duties of care owed to customers and business partners), sector-specific laws (e.g., regulations issued by financial industry regulators), and contractual obligations.

Canadian privacy laws regulate the collection, use, disclosure and retention of personal information by private sector organizations in the course of commercial activities in Canada. Those laws are based on internationally recognized *Fair Information Principles*, including the principles of Accountability, Safeguards and Openness.

- The Accountability principle provides that an organization is responsible for personal information in its possession or under its control, including information the organization has transferred to a third party (e.g., a CSP) for processing. An organization must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
- The Safeguards principle requires that personal information be protected by security safeguards appropriate to the sensitivity of the information. Those safeguards should include physical measures, organizational measures and technological measures to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.
- The Openness principle requires an organization to be open about its policies and practices with respect to the management of personal information. Organizations must be transparent about cross-border transfers of personal information to service providers in foreign jurisdictions.

The federal *Personal Information Protection and Electronic Documents Act* and the Alberta *Personal Information Protection Act* also impose security breach reporting, notification and record-keeping obligations on an organization that suffers a breach of security safeguards involving personal information under the organization's control.

Canadian privacy commissioners, regulators and industry associations have issued detailed guidance regarding the procurement and use of cloud services. For example, see BLG bulletins *Cloud Computing – Regulatory Guidance for Managing Risk*, *Cloud Services – Canadian Privacy Law Compliance*, and *Cybersecurity Guidance for Small and Medium Organizations*.

Guidance from the Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security (the "Cyber Centre") is the Canadian government's unified source of expert advice, guidance, services and support on cybersecurity for government, critical infrastructure owners and operators, the private sector and the Canadian public. The Cyber Centre has issued guidance to help organizations manage cyber risks, including risks associated with cloud services.

Risk management

In March 2019, the Cyber Centre issued *Cloud Security Risk Management* to help Canadian organizations manage the risks associated with cloud services. The guidance describes an "integrated risk management approach", based on existing standards, that can be applied to all cloud services. The risk management approach is comprised of nine steps: (1) perform security categorization; (2) select security control profile; (3) select cloud service and deployment models; (4) assess security controls implemented by the CSP; (5) implement security controls in the cloud service; (6) assess security controls implemented by the organization; (7) authorize operation of cloud service; (8) continuously monitor; and (9) maintain authorization.

Baseline controls

In March 2019, the Cyber Centre issued *Baseline Cyber Security Controls for Small and Medium Organizations* to help Canadian small and medium organizations maximize the effectiveness of their cybersecurity investments. The Baseline Controls reflect the view that organizations can mitigate most cyber threats through awareness and best practices, and can successfully apply the 80/20 rule – achieve 80% of the benefit from 20% of the effort – in the cybersecurity domain. The Baseline Controls recommend the following controls regarding cloud services:

- Require all CSPs share an SSAE 18 SOC 3 report that states that they comply with the Trust Service Principles (security, availability, processing integrity, confidentiality and privacy).

- Evaluate the organization's comfort level with how CSPs handle and access sensitive information (e.g., privacy and data-handling policies, notification processes when private data is accessed without prior authorization, destruction processes for data at the end of the contract, physical location and security of outsourced data centres, and physical location of outsourced administrators).
- Evaluate the organization's comfort level with the legal jurisdictions where CSPs store or use sensitive information.
- Encrypt all sensitive information stored in cloud services, and ensure secure access (e.g., using secure web browser connections) to the data.
- Ensure the organization's IT infrastructure and users communicate securely with all cloud services and applications.
- Ensure the organization's administrative accounts for cloud services use two-factor authentication and differ from internal administrator accounts.

For more information about the Baseline Controls, see BLG bulletin *Cybersecurity Guidance for Small and Medium Organizations*.

Benefits/risks assessment

In March 2020, the Cyber Centre issued *Benefits and Risks of Adopting Cloud-Based Services in Your Organization* to help organizations understand and manage the risks associated with using cloud services. The guidance reminds that "using cloud services does not automatically ensure that protections are applied to the assets that fall under these services", and that an organization's senior decision-makers "are still accountable for protecting the availability, confidentiality and integrity of IT services and information".

The guidance recommends organizations adopt a structured approach for managing risks associated with cloud services, including the following:

- Review the organization's existing IT resources and assess the value of new features and functionalities provided by using cloud services.
- Identify the value and sensitivity of the organization's information to help determine the information that the organization can store in the cloud and ensure adequate protection of sensitive business information and personal information.
- Review the Cyber Centre's security work regarding CSPs to find out more about a specific CSP's security controls and processes.
- Require a CSP to provide security certifications from independent auditors to confirm the CSP's security posture meets the organization's requirements.
- Use service level agreements with CSPs to define roles and responsibilities, document requirements for a CSP's performance, and outline financial penalties for underperformance.
- Review and manage security controls that protect the organization's assets in the cloud service.

The guidance reminds organizations to consider legal data residency requirements, and recommends that all organizations ensure that sensitive data is stored within Canada.

Technical matters

In May 2020, the Cyber Centre issued the following technical guidance for assessing and managing risks associated with cloud services: *Guidance on the Security Categorization of Cloud-Based Services*, *Guidance on Defence in Depth for Cloud-Based Services*, *Guidance on Cloud Security Assessment and Authorization*, and *Guidance on Cloud Service Cryptography*.

Guidance on the Security Categorization of Cloud-Based Services describes a process to identify and assess the risks presented by the use of a cloud service and to select a security control profile that adequately protects information and business activities. The guidance might also assist regarding the selection of an appropriate cloud deployment model (i.e., public, private, hybrid or community) and cloud service model (i.e., Software as a Service, Platform as a Service and Infrastructure as a Service).

Comment

Risk/benefit assessment

Generally applicable legal principles, statutory requirements and regulatory guidance support the view that an organization's decision to use a cloud service should be based on a documented assessment, informed by appropriate due diligence and expert advice (if necessary), as to whether the relative benefits of a specific use of a

particular cloud service justify the relative risks in light of all of the circumstances, including the organization's overall enterprise risk tolerance.

A risk/benefit assessment should be specific to each intended use of a particular cloud service. There are many different kinds of cloud services offered by many different CSPs, and each cloud service can be used in different ways for different purposes. In addition, various kinds of controls can mitigate the risks presented by the use of a cloud service. In some circumstances a specific use of a particular cloud service will be entirely appropriate, while in other circumstances the potential benefits of using the cloud service will not justify the risks.

A risk/benefit assessment should not be limited to IT issues or be prepared solely by IT personnel. An assessment should include risks and benefits to all aspects of the organization and its business, and involve the participation of representatives from all of the organization's relevant operational areas. In this context, risks and benefits are both absolute and relative concepts. The risks and benefits of a proposed use of a cloud service should be assessed realistically and in comparison with practicable alternatives (e.g., internal service, alternative cloud service, or no service). Alternatives to a cloud service will likely also have risks and benefits.

Cloud services contracts

An appropriate cloud services contract is a fundamental requirement for legal compliance. Canadian privacy commissioners, regulators and industry associations have issued detailed formal guidance regarding the kinds of provisions that should be in a cloud services contract, including data services contracts between related corporations. Informal guidance regarding cloud services contracts may also be found in privacy commissioner investigation reports.

In *Cloud computing for small and medium-sized enterprises*, the privacy commissioners acknowledge that it might be difficult for an organization to negotiate a cloud services contract that complies with all recommended requirements, particularly since many cloud service providers present "take it or leave it" contracts. Nevertheless, the privacy commissioners maintain that "any organization using a cloud service must carefully review the cloud provider's terms of service and ensure that the personal information it entrusts to the provider will be treated in a manner consistent with its privacy obligations under relevant privacy legislation", and conclude: "If you are not comfortable with what a particular cloud provider is proposing, you should not transfer personal information entrusted to you by your customers to that provider".

Oversight/monitoring

Canadian privacy commissioners, regulators and industry associations have emphasized that organizations should have a structured and documented program to monitor cloud services and oversee CSP compliance with contractual obligations. The nature and extent of appropriate oversight and monitoring will depend on the circumstances and the risks associated with the cloud services arrangement, and might include periodic reporting by the CSP, third party audits/certifications against accepted standards, and direct audits by the customer organization. A cloud services contract should provide the customer organization with appropriate oversight and monitoring rights. ■

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**.