Cloud Computing Guide

Best Practices & Checklist

for Law Practices in Saskatchewan

Law Society of Saskatchewan

Cloud Computing Guide – updated November 2023
This document is not intended to provide legal advice and is provided for informational use only.

Table of Contents

This document is not intended to provide legal advice and is provided for informational use only.

Overview

The use of cloud computing services by all manner of businesses including law firms has become pervasive. Based on a 2020 Law Society of Saskatchewan survey of legal practitioners in the province, at least 77.5% of those who responded, reported using some form of cloud-based service, for example:

Billing and accounting systems – Many legal billing and accounting platforms are now delivered through cloud-based client-server architecture;

Case management systems – Case management platforms are used to store and maintain client and file information, generate documents, and facilitate client-facing production electronic work product;

Marketing platforms – Social networks such as Facebook, LinkedIn, Twitter, etc. as well as Customer Relationship Management (CRM) systems, blog platforms and the like are used by many practitioners to track and maintain client relationships and new business pipelines;

Email and document hosting and storage – Email platforms including Microsoft Office365/Exchange, Gmail and others are most often hosted in the cloud, avoiding the need for maintenance of onsite server infrastructure. Similarly, more and more document management and retention systems are now delivered in cloud-based or hybrid architectures allowing for distributed access, storage and backup; and

File Sharing and Data Storage – Are cloud-based services such as OneDrive, Box, Dropbox, etc. that allow for the storage of a variety of file types (documents, pictures, videos, etc.), accessible and shareable from multiple platforms (phone, computer, tablet, etc.), from anywhere in the world.

Cloud services can provide several benefits to practitioners including reduced capital and maintenance costs for IT equipment and software, and the introduction of a pay-as-you-go operating model for only those services consumed. However, implementing cloud solutions requires practitioners to consider factors such as privacy, security, regulatory compliance, and service availability.

The purpose of this document is to provide practitioners with a set of best practices and a checklist to assist with evaluating or implementing cloud services. Practitioners should consider the questions and issues raised in this document when selecting or validating cloud service providers.

The following is a non-exhaustive list of topics of interests and concerns for practitioners to consider in assessing, their security posture and risk exposure, and the desirability of implementation of cloud-based products and services in their IT environments:

- Ensuring Compliance with Applicable Laws;
- Understand and Manage your Client Information;
- Understanding Cloud Security Risks;
- A Note of Caution on Consumer Cloud Services; and
- Cloud Service Agreements.

This document is not intended to provide legal advice and is provided for informational use only.

Cloud Best Practices

Ensuring Compliance with Applicable Laws[1]

Through the example of privacy laws and regulations we illustrate below some of the analysis practitioners should undertake when trying to determine their compliance obligations when outsourcing data storage and processing to Cloud Service Providers (CSP).

The laws and regulations affecting your practice extend beyond those promulgated within the province of Saskatchewan. For this reason, practitioners will need to be mindful of federal laws governing specific entities, sectors, or employees (e.g., *The Privacy Act*), and international laws and regulations which are extra-territorial in nature (e.g., General Data Protection Regulation (GDPR)).

The following questions can assist practitioners in determining their compliance obligations:

- What is the geographical location of the practitioner/employees/ subcontractors having access to the records?
- What is the geographical location(s) of the client?
- What is the geographical location where the cloud service is being provided (Canada, US, International)?
- Does the data cross provincial or national borders – whether for processing or storage?
- Is the client private, public, or a non-for-profit?
- Is the client's industry federally regulated?
- Does the client, the client's regulator or its industry generally, have rules for data localization (e.g., requiring storage and processing in Canada)?

Understand and Manage your Client's Information

In the course of representing clients, practitioners will often receive, process, and generate significant amounts of confidential and sensitive information for, or on behalf of, those clients. For example, a client record may contain personal information and other sensitive data such as financial information, intellectual property and trade secrets, information about mergers, acquisitions, or other strategic or competitive business information. Practitioners may also receive or generate additional sensitive and confidential information (e.g., through litigation, regulatory processes and similar proceedings) carrying particular confidentiality (e.g., blueprints in accordance with certain regulations) or legal privilege obligations (e.g., disclosures provided in exchange for protective covenants).

[1] While this document does provide some high-level guidance and reference to certain laws, it is not intended to provide a fulsome review of all legal and compliance obligations which may apply to your adoption and use of cloud services, nor is it intended to replace experienced legal and technology security expertise and advice. Further, the Law Society of Saskatchewan may update its *Rules* and this record from time to time in order to ensure the appropriate identification and treatment of technology and information risk by Members.

Client information may reside in obvious places such as desktop computers, laptops, and servers, but it may also reside in other, less expected locations, such as systems backups, mobile devices, and even the hard drives of photocopiers and printers.

Regardless of how this information is obtained and where it resides, it is important that it is protected from unauthorized access, disclosure and breaches throughout the information lifecycle (e.g., from collection to destruction). In order to effectively safeguard information, practitioners should be familiar with:

a) the different types of information in their custody and control,
b) where the information resides, and
c) the different safeguards and processes that are being used to protect the information.

These considerations apply irrespective of whether the information is located in a physical file, on a practitioner's private server or on a CSP's server. However, a key question to consider before moving sensitive or confidential client information to the cloud is "does the cloud offer the same or greater security to protect the information as an on-premise/in-house solution."

Practitioners should also be mindful of the fact that moving a client's information to the cloud will not relieve them of their legal, regulatory and ethical obligations to ensure that the information is protected from unauthorized access, disclosure or loss. In other words, even though the responsibility to store or process the information may be outsourced to a third party, the accountability for its safekeeping always remains with the practitioner.

Good information management processes can be a competitive differentiator. Practitioners should also consider the impact of client expectations and requirements as well as individual interpretations of privacy. What is acceptable to one client may not be acceptable to another, regardless of specific regulatory requirements.

Managing and protecting client information can be time consuming and can often feel overwhelming for some practitioners. However, there are a variety of services and technologies that practitioners can obtain to help assist with these processes.

Understanding Cloud Security Risks

While closely related, security and privacy are not synonymous. In fact, information can be highly secured while violating a client's privacy. For example, information may be encrypted end to end, but the information is not being used for its original purpose without the consent of the client or the information is being retained indefinitely (e.g., long after it has fulfilled its intended purpose).

The security measures undertaken by CSPs may be more robust and powerful than what a practitioner is capable of achieving "in-house". Indeed, in many instances, the information stored with a CSP may be safer than the information stored in a practitioner's computer hard drive.

Nonetheless, the introduction of cloud services can also introduce or amplify existing security issues. The absence of good cloud security can make a practitioner vulnerable to security risks that can erase any gains made by the switch to cloud technology.

When considering a migration to a cloud service, practitioners should understand their exposure to security threats and vulnerabilities so that steps can be taken to address and mitigate those risks. Cloud security risks are inevitably a matter which will require the input of a third party with information governance and security expertise. When engaging this expertise, practitioners should consider the following, as outlined by the Cloud Security Alliance[2]:

1. **Data Breaches –** sensitive, protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so.
2. **Misconfiguration and Inadequate Change Control** – where computing assets are set up incorrectly leaving them vulnerable to malicious activity. Some common examples include: unsecured data storage containers, excessive permissions, default credentials and configuration settings, and disabling standard security controls.
3. **Lack of Cloud Security Architecture and Strategy** – the failure to implement and/or modify appropriate security architecture and strategies when moving to the cloud. Changes are often required to an organization's existing security controls/processes when migrating to the cloud, and these changes are frequently overlooked.
4. **Insufficient Identity, Credential, Access, and Key Management** – inadequate protection of credentials, lack of regular automated rotation of passwords and certificates, failure to use multifactor authentication, failure to use strong passwords.
5. **Account Hijacking** – attack methods such as phishing, fraud and exploitation of cloud service vulnerabilities.
6. **Insider Threats** – a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or cloud service.
7. **Insecure User Interfaces (UIs) and Application Programming Interfaces (APIs) –** CSPs will often provide a set of UIs and APIs to allow their customers to manage and interact with cloud services. These interfaces must be designed to protect against both accidental and malicious attempts to circumvent security policy; poorly designed APIs can lead to misuse or a data breach.
8. **Weak Control Plane –** a "control plane" is the part of a network that controls how data is forwarded. Moving from a data centre to the cloud can create challenges for sufficient data storage and protection as the user must develop new processes for data duplication, migration, and storage. A control plane is used to address these issues however a weak control plane can result in data loss, either by theft or corruption; users may be unable to protect their cloud-based business data and applications.
9. **Metastructure and Applistructure Failures** – CSPs routinely reveal operations and security protections that are necessary to implement and protect their systems successfully. These protections are incorporated in the "metastructure layer" for the

[2] Top Threats to Cloud Computing: Egregious Eleven | CSA (cloudsecurityalliance.org)

service provider. Failure in this model can offer attackers an opportunity to disrupt cloud customers by interrupting confidentiality, integrity, or availability of the service.

10. **Limited Cloud Usage Visibility** – limited cloud usage visibility occurs when an organization does not possess the ability to visualize and analyze whether cloud service use within the organization is safe or malicious.
11. **Abuse and Nefarious Use of Cloud Services** – misuse of cloud service-based resources include launching Distributed Denial of Service (DDoS) attacks, email spam and phishing campaigns; "mining" for digital currency; large-scale automated click fraud; brute-force attacks of stolen credential databases; and hosting of malicious or pirated content.

Mitigating risk when using cloud services requires an awareness of the sensitivity of the information flowing through or housed in the cloud environment, together with consideration and an alignment between "*people"*, "*process"*, and "*technology"* as detailed below:

People

A highly secure cloud service can still be exploited through inappropriate use or management of a CSP. Inappropriate use or management of CSPs can be unintentional as security risks may not be obvious. Indeed, much attention is given to the threats posed by malicious third parties (e.g., hackers), but the consequences of inattention, a lack of due diligence or carelessness can be equally as catastrophic.

Every user needs to know and understand potential security risk types as well as how to avoid, mitigate and respond to a security event should a response be required. It is advisable for practitioners to establish periodic ongoing training on potential security risks, security responses and good data management, and to keep up with emerging technologies and the evolving cyber threat landscape. As well, training should be provided on how to securely use technologies that do not increase the chance of someone gaining access to a practitioner's cloud services or data (e.g., phishing, social engineering, etc.).

Process

A series of repeatable processes should be established and documented, together with organizational policies detailing accountabilities to ensure compliance and consistency. The policies should be documented in a way that can be clearly communicated to those within the practitioner's organization/practice as well as to clients who trust their data is secure.

Good security policies and processes can be enforced by having good cloud security controls. The following security controls should have policies and processes documented for each:

1. **Deterrent** – intended to discourage nefarious actors from attacking a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. Inside attacks are a source of risk for cloud providers, so an example of a deterrent control could be a CSP conducting criminal background checks on employees.
2. **Preventive** – strengthen the cloud service against security incidents by reducing vulnerabilities (e.g., strong passwords, multifactor authentication, etc.).

3. **Detective** – detect and respond appropriately to security incidents that occur. In the event of an attack, a detective control will help identify the nature and extent of the compromise and inform the measures to contain, correct and recover from an incident (e.g., systems alerts, monitoring of access and event logs which are similar to audit trails etc.).
4. **Corrective –** reduce the consequences of an incident, normally by limiting the 'blast radius' which may result from an incident (e.g., auditing the existence and sufficiency of controls, conducting penetration tests and addressing vulnerabilities).

Technology

There are a number of technologies that should be used to deter, prevent, detect and correct risks and security threats; these technologies also support connecting to and using the cloud service through a device such as a laptop or phone and over the internet. Some CSPs implicitly provide security-based technologies as part of their service.

Practitioners will have different technology requirements based on factors such as their office size and the sensitivity of the data they responsible for, as such, practitioners will need to identify and deploy technology that is right for them. The technology chosen must meet or exceed the risks and vulnerabilities associated with the sensitivity of the information entrusted to the firm. Practitioners should also identify the risks inherent with the technologies and tools used to administer the business (e.g., payroll) and to deliver client services (e.g., document management).

While technology requirements can be unique for each practitioner, it is imperative that a third party with information governance and security expertise is engaged to assess and adopt appropriate security safeguards.

Continual Review

All of these concepts (People, Process, and Technology) should be continually reviewed as part of responsible risk management.

A Note of Caution on Consumer Cloud Services

Some CSPs offer solutions like email, word processing, spreadsheets, and online file storage at no direct cost to the user. Due to the low cost and ease-of-use, it can be tempting to use consumer cloud services for business use. However, there is a higher likelihood that data on a consumer client service (free services) may be at risk as freeware versions often do not have the same data governance and security controls made available through the paid versions. Business cloud services are also typically purpose-built for availability, data privacy and security while also providing additional service options that are not present in consumer cloud services.

Periodically Review Use of Cloud Services, Data and Applicable Laws (including Privacy)

Cloud technology as well as privacy regulations are constantly changing and evolving. Understanding those changes and their applicability to your practice can be a challenge especially if the benefits of a cloud service are already being realized. With any change, risks from change need to be identified and actioned.

International laws and regulatory requirements may also impact your data, particularly where that data concerns a client resident in another country. For example, while in theory the GDPR applies to data of citizens of the European Union (EU), it is also possible that non-EU entities could also be affected. As such, it is critical to engage appropriate foreign counsel in these cases to best ensure compliance.

In light of the foregoing, it is recommended to set up processes for regular review of:

- All software that processes or stores your data;
- All hardware and other devices with access to your data;
- The nature, type and location of the data that is already stored on that cloud service; and
- New and existing legislation and regulatory guidance.

Cloud Service Agreements

Defining Cloud Service Agreements

Cloud service agreements are the “terms of use” or “terms of service” for CSPs to provide cloud services to users. They will often consist of several related, but separate, legal documents. While the exact naming conventions chosen by a given provider differ, the critical agreements for most providers are:

- **Service Terms –** These are the primary terms of use/service employed by the CSP. They will discuss the scope of services offered, privacy and security matters, intellectual property ownership, indemnification, limitations of liability and (most often very limited) representations and warranties.
- **Service Level Agreements (SLAs) –**These are performance standards set by the CSP which speak to the availability of the cloud services. At its core, an SLA will discuss how often (on a percentage basis) the cloud services will be available (“uptime”), as well as when it is permissible for the cloud services to be unavailable for events such as maintenance (“downtime”). Consequently, SLAs are critically concerned with metrics (for example, being available 99.999% measured on a “365/24/7” basis). By contrast, you should watch for “service level objectives”, which are nothing more than high level objectives and not an agreed upon level of performance.
- **Support Services Agreements (SSAs) –**These set out the scope and availability of support, warranties, and maintenance associated with the cloud services. They will typically address matters such as response times, updates, unsupported services, on-site maintenance (where applicable), and the term or duration of the commitment. You should watch for the manner in which service interruptions are classified (and the related efforts of the CSP to remediate those interruptions). For example, a complete failure of a service may require remediation within several hours, whereas an

interruption only impacting a limited set of users (or only specific functions of the services) may require remediation within several days. The response form can also be important to observe (e.g., by phone, by text, by email).

Getting Ready for Cloud Services

It is critical to understand that cloud service agreements are quite often not open to meaningful negotiation. The CSP is often a large incumbent (e.g., Microsoft) or has simply adopted a low-risk tolerance based on the fact that these services are deployed to thousands, if not millions, of users. To such a large CSP, assuming any material risk for any customer is unacceptable. As a result, practitioners should consider several non-legal questions before engaging in protracted negotiations on the cloud services agreements:

- Is a “mission critical” aspect of the practitioner’s practice being outsourced? For example, contrasting practice or document software management with calendar scheduling software.
- How long is it acceptable for the cloud service to be unavailable? For example, consider the financial implications to practitioners of lengthy downtime of email and document management services, as contrasted against legal research services.
- Is the data (which is at the heart of the cloud services) managed internally or through an existing cloud provider? If internal, practitioners will want to be concerned around the onboarding timelines and what procedures will need to be in place to ensure a seamless transition. If the latter, practitioners may be able to engage in some measure of playing one CSP off another as part of negotiations.
- What is the state of the practitioner’s internal IT expertise? If the expertise is low to non-existent, there will be much more dependency on the CSP. In that instance, it may also be warranted to engage a third-party IT consultant or expert solely to assist with integration and onboarding of this new cloud service (as well as potential negotiation with the CSP).
- What self-help remedies and protocols are the practitioners currently employing within the office/firm? These might include, for example, internal policies around accessing data, encryption, back-ups and recovery processes, employee training, and cybersecurity insurance. Not having robust internal remedies and protocols makes practitioners more beholden to the CSP.
- What is the cost of the cloud service relative to other software deployed by the practitioner as well as other practice management expenses of the firm? While not a comment unique to cloud service agreements, if the value of the arrangement is relatively low (and the data in question is not highly sensitive), then protracted negotiations are unlikely to be warranted.
- Is the cloud service being deployed for all practitioners at the firm or only for specific practitioners? If the latter, it will be important to understand the specific needs of those practitioners and whether the cloud service agreements need to control for any nuances of those practice areas.
- What is the practitioner’s comfort level with the CSP? For larger incumbent CSPs, there may be concern around responsiveness and willingness to modify services to accommodate specific firm needs. For smaller CSPs, there may be concerns around maturity and whether the CSP is adequately capitalized to endure the early stages of

a cloud business. Additionally, have the practitioners been provided references and had substantive discussions with existing law firm clients of the CSP?

- How difficult will it be for practitioners to end their relationship with the CSP? What obligations does the CSP have in that situation? Practitioners should be specifically interested in ensuring the safe return of client data in a reasonably short time frame post-termination, in a format usable by the firm, and at a reasonable cost. At times, more extensive post-termination obligations of the CSP can be negotiated in the form of a transition services agreement.

Diligence and Negotiations on Cloud Services

The questions posed above (among others) and the actual negotiation of the cloud service agreements is a multi-step exercise (which may unfold contemporaneously):

1. Diligence on Existing Controls of CSP – Review existing physical, technical, and administrative controls employed by the CSP. Examples of each include:

    a. Physical – Limiting physical access to premises where data is stored, locks, safes, vaults, guards, and sensors.

    b. Technical – Firewalls, intrusion detection software, access control software, antivirus software, passwords, smart cards, and encryption processes.

    c. Administrative – Personnel management, employee use policies, training, discipline, and informing people how to conduct day-to-day operations, and disaster recovery and business continuity plans.

    The CSP should be providing practitioners with details of these items, typically in the form of written policies. Perhaps most critically, practitioners should be requiring references from the CSP and making efforts to have substantive conversations with those references.

2. Cloud Service Agreement Modifications – As previously noted, there is unlikely to be wide latitude for negotiations on the cloud service agreements themselves. However, practitioners should pay particular attention to:

    a. Service levels and what percentage uptime is being offered by the CSP.

    b. When scheduled maintenance will be occurring.

    c. Whether the CSP will indemnify practitioners for events such as:

        i. a cybersecurity event and related data loss or corruption,

        ii. allegation that the CSP’s services infringe the rights of third parties,

        iii. breach of confidentiality covenants,
        iv. breach of regulatory requirements, and

        v. failures to implement adequate security safeguards.

    d. The limitation of liability cap (often set at the last 12 months of fees paid by practitioners to the CSP).

e. The level of security safeguards being offered by the CSP (often framed minimally as "industry best practices" but may be referenced instead to international security standards such as ISO 27001, NIST, SOC II, which are certifications that address data security and privacy challenges for businesses).

Again, while practitioners may not be successful in modifying the CSP's base terms, the responses to the inquiries on these items may be quite illuminating.

3. Practitioner Accountability - As with any outsourcing arrangement, practitioners must bear in mind that the transfer of responsibilities of data storage and processing does not absolve them of their accountability to govern, control, and secure their data and records. Some strategies for ensuring accountability may include:

a. Cybersecurity insurance.

b. Hiring either internal IT expertise or retaining the services of an external IT consultant.

c. Adopting internal policies around use and access of data and setting up ongoing training for firm members[3].

d. Deploying technical safeguards such as robust passwords, multi-factor authentication, virtual private networks (VPNs), and single sign-on.

Ongoing Review and Renewal of Cloud Service Agreements

Once the cloud service agreements have been settled, practitioners should ensure that there is a process for ongoing review of those agreements. CSPs will continually update these agreements, often without meaningful attempts to notify users. Specifically, when cloud services are coming up for renewal, practitioners should be making determinations as to whether new terms should be included as part of a renewed arrangement with the CSP.

[3] Two useful resources for consideration of security controls and general risk analysis include the Baseline Cybersecurity Controls set by the Canadian Centre for Cyber Security, as well as the Treasury Board of Canada's Guidance Document: *Taking Privacy Into Account when Making Contracting Decisions.*

Cloud Checklist

A. Compliance with Applicable Laws

Jurisdiction

Commentary
Consider locally applicable privacy laws as well as those of extra territorial application. Ensure that you remain informed about the evolving landscape of applicable laws regulating the collection, processing, and storage of personal information – including those that apply to your firm; your clients; and your service providers.

			YES	**NO**	**USER NOTES**
1	**Do you have clients in the following geographical locations outlined below?**				
			YES	**NO**	**USER NOTES**
2	**Do you currently or plan to use cloud services being provided from the jurisdictions below?**				
a	Saskatchewan	e.g., The Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal statute that will apply to most private-sector businesses in Saskatchewan. Notably, public sector or regulated entities will need to consider the applicability of The Freedom of Information and Protection of Privacy Act (FOIP) which applies to “government institutions”; The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP), which applies to “local authorities”; and The Health Information Protection Act (HIPA), which applies to “trustees” under that legislation.			
b	Elsewhere in Canada	In addition to PIPEDA, several jurisdictions in Canada have their own legislation governing the collection and use of personal information e.g., B.C., AB, QC Similar to the section above, public sector or publicly regulated entities will need to consider the applicability of other legislation which may inform the adoption and use of cloud services.			
c	United States	Various federal and state regulators and laws govern the protection of personal information (e.g., The Federal Trade Commission, the California Consumer Privacy Act). See for example, FISA, USA Patriot Act, USA Freedom Act			
d	European Union	The General Data Protection Regulation (GDPR) is a regulation that harmonizes national data privacy laws throughout the EU and has extra-territorial application when an entity is storing or processing the personal data of EU citizens.			
e	Other	An increasing number of jurisdictions have their own privacy laws which may implicate the collection, storage, or processing of the data collected, stored or processed by or on behalf of your firm.			

Client Sectors

Commentary
Consider the application of government or industry regulations that may impose requirements for data localization in specific jurisdictions or prohibit storage or processing of information in particular jurisdictions. Disclosing the geographic location(s) of cloud services is not only transparent, but it will help support client awareness and compliance.

3	**Do you have clients operating in the following sectors?**	**YES**	**NO**	**USER NOTES**
a	Healthcare			
b	Insurance			
c	Accounting			
d	Banking and related investment or financial services			
e	Information technology or security			

		YES	**NO**	**USER NOTES**
4	**Do you have clients with their own specific requirements for the storage, information residency or communication of records?**			
a	Expanding on (4) above, do clients require or prefer certain communications or document exchange processes and protocols?			

Commentary (Question 5)
Having the ability to determine the sensitivity of information in your various repositories allows the ability to ensure that security controls are commensurate with the sensitivity of the information in a particular environment. Without this awareness, organizations will over or under protect their information.

		YES	**NO**	**USER NOTES**
5	**Do you review and categorize personal or sensitive client and employee data, as required by the identified privacy legislation?**			

Commentary (Question 6)
While the appropriate retention and destruction of records should be standard practice, privacy laws may also require the deletion, correction or other modification to personal information in your custody or control (e.g., the personal information of your employees).

		YES	NO	USER NOTES
6	**Does your practice have a process to change or remove client data to meet compliance requirements, if required?**			

Commentary (Question 7)
Generally, you will have an obligation to understand how vendors may access and use data (particularly personal information) and to communicate with affected individuals (e.g., your clients or employees) about how their information may be used, shared and to whom it may be disclosed.

Cloud service contracts will specifically require licensees to comply with applicable privacy laws and include a Rep and Warranty concerning your authority to process or store personal information in their environment.

		YES	NO	USER NOTES
7	**Does your client data meet regulatory compliance requirements for the legislation identified above?**			
a	For example, do you have the client’s permission to collect and retain their data for its original purpose?			
b	Have you acquired consent if client data is to be retained after its original purpose?			
c	Do you have client consent if their data is being processed or disclosed for a secondary purpose?			

		YES	NO	USER NOTES
8	**Do you have any data being processed or stored outside of Canada?**			
a	If so, have clients been informed?			
b	Have clients provided consent where required by law?			

B. Cloud Security & Risk

Commentary
Security in the cloud is vitally important. Online databases of information are attractive targets for cybercriminals and have proven to be difficult to protect both in terms of the technical controls and your “human firewall” – the personnel supporting your business processes. You are obligated to protect its data with safeguards appropriate to the sensitivity of the information.

Commentary (Question 1)
Do not assume that the provider’s general terms of service or policies will be adequate to establish such restrictions, review them carefully.

Look for language that may permit the provider to access, analyze or sell your data or metadata for its own purposes or in any other way. Pay particular attention to language about the aggregation of data or commitments to anonymize data to ensure that you understand the risk of potential re-identification of data to ensure that it is, in fact, permanently de-identified to protect your employees and clients from potential harm.

		YES	NO	USER NOTES
1	**Have you read the cloud provider’s ‘click-thru’ and other agreements relating to the services?**			
		YES	**NO**	**USER NOTES**
2	**Do the service contracts clearly state who you can rely on for support and maintenance?** **Considerations for support:**			
a	Do the times of available support match your typical operating hours?			
b	Is there emergency contact information?			
c	Does the method of communication (phone, email, text) match your requirements?			
d	Is there an extensive knowledge base on the cloud service for self-help and support?			

		YES	NO	USER NOTES
3	**Does your cloud provider meet your backup and recovery requirements for:**			
a	Immediate data recovery with no data loss			
b	Data archiving			
c	Disaster recovery			

Commentary (Questions 4 to 7)
Consider appropriate parameters for restricting access and use of data that is appropriate for the context and sensitivity of the information.

Ensure that appropriate authentication/access controls are enabled to your systems (e.g., multi-factor authentication is recommended) and generally, the level of authentication should be commensurate with the risk to the information (e.g., personal information or other sensitive information such as competitive business information, trade secrets etc.). Ensure there are procedures and technical controls to manage who has access rights to the data, particularly personal information.

Consider the extent to which your data will be segregated or stored in the same database as information from the cloud provider's other clients (segregation is preferred and sometimes required).

In terms of the service provider's access and your own personnel, work to apply the principle of least privilege (provide no more access or authorizations than are strictly necessary to perform required functions). For example, ensure access to personal information is only granted to those who need it to do their job and when such access to personal and sensitive information is enabled, ensure logging capabilities and audit trails are available.

		YES	NO	USER NOTES
4	**Are there clear controls limiting access to and further use of your data by the vendor and its sub-contractors?**			
		YES	**NO**	**USER NOTES**
5	**Do you have the client's permission to retain their data for its original purpose?**			
		YES	**NO**	**USER NOTES**
6	**Have you acquired client consent if client data is to be retained after its original purpose?**			
		YES	**NO**	**USER NOTES**
7	**Do you have client consent if their data is being disclosed for a secondary purpose?**			

Commentary (Question 8)
Understand what type of encryption method is being used and identify where data is encrypted or unencrypted at each stage (e.g., data in transit, data at rest). Conduct an assessment of the risks associated with any lack of encryption. Determine if the encryption method is adequate and the access to encryption keys is properly managed.

		YES	NO	USER NOTES
8	**Does the cloud service provider have multiple types of security?**			
a	Company-based security (intrusion detection and prevention, spam and virus filters, etc.)			
b	Access-based security (based on identity or role of an individual in your organization)			
c	Transport-based security (such as Virtual Private Network or VPN, Secure Socket Layer or SSL tunneling or encryption)			
d	Multi-Factor/Two-Factor Authentication			
e	How will your data be encrypted in transit and at rest when using the service?			

Commentary (Questions 9 and 10)
Consider applicable compliance obligations (see above) which are informed by your client’s geographical location(s) and industry sectors.

Seek to negotiate data localization in Canada, where required. Where not required, you may wish to evaluate which of the service provider’s locations offer the best service and support.

		YES	NO	USER NOTES
9	**Will your data be processed and/or stored outside of Canada?**			
		YES	**NO**	**USER NOTES**
10	**Does all your client data meet regulatory compliance requirements for the identified regulatory acts?**			
		YES	**NO**	**USER NOTES**
11	**Does the service provider have contract language regarding the confidentiality, integrity and availability of your data?**			

a	Does the cloud service meet your requirements for availability?			
b	Is there an extra cost to ensure sufficient cloud service availability to meet your needs?			
c	Consider whether to validate your cloud provider's actual availability history to ensure it meets your availability requirements.			
d	Can the cloud service scale (increase or decrease) based on demand?			
		YES	**NO**	**USER NOTES**
12	**Does the service provider have contract language regarding compliance with applicable laws?**			

Commentary (Question 13)
The ability to sub-contract all or part of the service increases risk. Accordingly, seek to understand when and how sub-contracting is permitted and limit the number and location of sub-contractors wherever possible. Find out how sub-contracting works if permitted in the contract and consider whether you can control the ‘when’ and ‘who’ of subcontracting (these can often be managed by having a pre-qualified or approved list of subcontractors).

If possible, seek information about the subcontractors (e.g., SOC II Type II reports) if they may have access to your data or security controls for the service.

		YES	**NO**	**USER NOTES**
13	**Does the cloud service provider use other 3rd party cloud services (‘clouds of clouds’)?** **If yes:**			
a	Is the location of the 3rd party cloud service provider within Canada?			
b	Does the 3rd party cloud service provider fall under the original cloud services contractual terms and conditions?			
c	Does the 3rd party cloud service provider meet the identified regulatory requirements?			
d	Is the cloud service provider required to give notice if contemplating contracting out to other providers?			
e	Have your clients been informed of the geographical location of their data, what data is being used/stored, and their options to opt out?			

		YES	NO	USER NOTES
14	**Does the cloud service provider use a sub-contractor?** **If yes:**			
a	Is the location of the sub-contractor within Canada?			
b	Does the sub-contractor fall under the original cloud services contractual terms and conditions?			
c	Does the sub-contractor meet the identified regulatory requirements?			
d	Is the cloud service provider required to give notice if contemplating contracting out to sub-contractors?			
e	Have your clients been informed of the use of sub-contractors and their options to opt out of the cloud service?			

Commentary (Questions 15 to 18)
Service disruptions and outages are a predictable consequence of using technology solutions. Most cloud contracts contemplate these issues with separate Service Level Agreements (SLA) which govern the relationship between you and the service provider and provide the minimum levels for each element of service provided allowing you to anticipate outages, timelines to return to operations, as well as potential available remedies. Practically speaking, the remedies will not compensate for business disruption, consequently, your practice should have alternative business processes to allow for temporary and continued operations when disruptions occur.

Ensure that service standards and maintenance commitments for system performance, security management, data management and personal information protection are sufficient to meet your needs.

Service levels should be well understood by your technical support team and ‘translated’ to allow you to anticipate the potential impact on your operations. Pay particular attention to how uptime and downtime is calculated to know if scheduled maintenance is included in downtime.

		YES	NO	USER NOTES
15	**For how long can your practice continue to operate if the cloud service is unavailable?**			

		YES	NO	USER NOTES
16	**Do you understand the vendor’s data backup processes and are you satisfied with service standards?**			

17	**Do you have documented manual/backup processes in place to operate your practice while the service is unavailable?**	**YES**	**NO**	**USER NOTES**
18	**Have you read the cloud provider's SLA?**	**YES**	**NO**	**USER NOTES**
19	**Does your cloud service provider require planned outages for maintenance?**	**YES**	**NO**	**USER NOTES**
a	Will you be given adequate notice for maintenance periods?			
b	Are the cloud provider's schedule and duration for maintenance acceptable?			
c	Does your cloud provider need you to test the cloud service before, during, or after the maintenance period?			
20	**Are availability, performance, and bandwidth representations spelled out in the SLA?**	**YES**	**NO**	**USER NOTES**
a	Are there penalties for your cloud provider not meeting their SLAs?			
21	**Will the cloud service provider give your firm notice when the SLA agreement and other underlying policies are changed?**	**YES**	**NO**	**USER NOTES**
22	**Does the SLA ensure intellectual property rights and/or ownership rights to your data are not transferred during the life of the contract as well as after?**	**YES**	**NO**	**USER NOTES**
23	**Is there a dispute resolution method or process in the cloud provider’s SLA?**	**YES**	**NO**	**USER NOTES**

This document is not intended to provide legal advice and is provided for informational use only.

Commentary (Questions 24 and 25)
It is recommended that you have some measure of oversight over the cloud provider’s policies, practices and service standards. Ensure the cloud provider logs all accesses and uses of information. Audits should include inspection of access logs and confirmation that physical locations where information is processed and stored are inspected. Verify the vendor’s practices and procedures to ensure that it is handling personal and sensitive information in accordance with the agreements and request evidence of effective auditing and timely response to security incidents. Where relying on third-party audits, ensure that they are conducted by reputable experts and available on a predictable schedule.

		YES	NO	USER NOTES
24	**Does your cloud service provider have a means to monitor for and report abuse of the cloud service (e.g., Denial-of-Service) attacks?**			

		YES	NO	USER NOTES
25	**Do you plan (and have the ability) to audit or review audits of the cloud provider's data security performance?**			

Commentary (Question 26)
When outsourcing data storage and processing to a third party, consider whether the cloud service provider has sufficiently demonstrated accountability for its privacy and confidentiality obligations. Where risk or responsibilities do not transfer, consider how your practice can establish compensating controls to augment those provided by the cloud service provider. For example, some service providers may make no commitments with respect to personal information on the assumption that personal information will not be transferred. Consequently, it is necessary to ensure that only de-identified data is shared with such a provider.

		YES	NO	USER NOTES
26	**Have you read the cloud service provider’s Privacy and Confidentiality Agreement?**			

Commentary (Question 27)
In addition to your own technical and organizational measures to manage the risks of accidental or deliberate loss, or unauthorized access or disclosure of information, ensure there are provisions in the agreement that specify when you will be provided with notification in the event of a breach of security controls that may compromise your data. Gather sufficient information to understand how security breaches will be addressed. The contract should be clear about when the service provider reports on breaches.

Ask how the cloud provider has responded to past security breaches. Are you satisfied with the cloud provider’s response? Do you need more information to understand how security breaches will be addressed?

You may wish to be informed of all incidents, even if it is likely that you, your clients or personnel are not negatively impacted by the incident.

		YES	NO	USER NOTES
27	**Do you understand how the service provider will detect and respond to security breaches, and will you be notified in the event of security breaches that could affect your data?**			
a	What is the process?			

Commentary (Questions 28 and 29)
In the event of an attack, it may be possible to recover from the service provider (see below).

Cloud agreements will allocate liability between the parties for the wrongful disclosure or loss of data. The contract should provide the ability to hold the cloud provider liable for its acts, omissions or gross negligence that resulted in the loss or disclosure of data.

Many agreements will seek to reduce or totally eliminate the cloud provider’s liability to you. The sensitivity and criticality of the data should guide your decision to amend contract terms that limit the cloud provider’s liability.

		YES	NO	USER NOTES
28	**Does your cloud provider carry liability insurance and cyber risk insurance associated with ransomware attacks?**			

		YES	NO	USER NOTES
29	**Does your cloud provider have a policy and process to handle ransomware attacks?**			

Commentary (Questions 30 and 31)
Providers of technology solutions will typically limit their exposure to risk by having rigid Limitations of Liability in their agreements. As a consequence, all potential losses may not be recoverable.

		YES	NO	USER NOTES
30	**Is the cloud provider required to compensate you for losses as a result of using their service?**			

		YES	NO	USER NOTES
31	**What are the Limitations of Liability associated with the Services?**			

Commentary (Question 32)
Business continuity plans should be clearly documented in the contract.

To identify commitments, look for contract language about backups, restoration and return to operations. In the case of ransomware attacks, complete data recovery will, at best, be costly and time consuming; at worst, it may be incomplete. And consider based on the criticality and sensitivity of the data whether you may require that your data be “safe harboured” (e.g., where a copy of your data is stored securely by a third-party provider to mitigate against data loss or the inability to access data via the service provider.) (see below)

		YES	NO	USER NOTES
32	**Can your cloud provider recover your data in the event your data and/or cloud service is no longer available to you?**			

33	**Is your cloud service provider able to retain and/or archive required data for the legally specified period (e.g., law practice accounting information)?**	**YES**	**NO**	**USER NOTES**

Commentary (Questions 34 – 41)
As with any contract, have an exit strategy which, in this case, permits the efficient transfer of data back to you or to your new service provider(s) and require that your cloud provider securely delete your data and particularly, all personal information, within reasonable and specified timeframes.

What will happen with your data upon contract expiration or termination (including if the provider ceases to operate)? What can you do with backed-up data in such cases? Consider, for example, that the cloud provider may use a proprietary application or system to organize and manipulate your data. Backed-up data may not be that useful if you are unable to export/migrate it into another product and maintain/regain data relationships. For this reason, confirm what format the data will be in when it is stored and used in the cloud and provide your requirements in advance for data migration in the event of termination or expiration of the contract.

34	**Do you have a documented cloud exit strategy in the event you wish to move away from a cloud provider?**	**YES**	**NO**	**USER NOTES**
35	**Can you terminate the cloud service without penalty?**	**YES**	**NO**	**USER NOTES**
36	**Can your data be easily moved from one cloud provider to another?**	**YES**	**NO**	**USER NOTES**
37	**Is the cloud provider required to provide transition support if the service is terminated?**	**YES**	**NO**	**USER NOTES**
38	**Will the cloud service provider provide your data in a format that can be moved to another cloud provider?**	**YES**	**NO**	**USER NOTES**

This document is not intended to provide legal advice and is provided for informational use only.

39	Will the cloud provider retain your data for an extended period of time in the event your contract with the cloud provider ends?	YES	NO	USER NOTES
40	Do you know the length of time it would take to migrate data from one cloud service provider to another and is that time acceptable?	YES	NO	USER NOTES
41	Can your data be sanitized from the cloud provider in the event of a termination?	YES	NO	USER NOTES

C. Information Management and Hygiene in your Practice

Commentary
Have you identified what data will be placed in the cloud and its corresponding (a) sensitivity and (b) criticality to your practice? (e.g., credit card data, personal information, confidential or other sensitive information will have particular requirements).

1	**Do you have sufficient Internet bandwidth to run the cloud application with acceptable performance?**	**YES**	**NO**	**USER NOTES**
2	**Do you have a secondary internet connection should the primary internet connection not be available? (e.g., cellphone as a wireless hotspot)**	**YES**	**NO**	**USER NOTES**
3	**Do you have a requirement to integrate a cloud service with another cloud service or internal office system?**	**YES**	**NO**	**USER NOTES**
a	Does the cloud service integrate with your other office systems including other cloud services if required?			
b	Do you know the level of IT support that will be required to support cloud service integration?			

Commentary (Question 4)
Ensure that you have procedures in place in the event of an outage to ensure business continuity and to prevent data loss.

Some organizations encrypt personal and other sensitive information before it is sent to the cloud provider. Generally, the need for encryptions is determined by the sensitivity of the data (e.g.,. personal information, competitive business information and other sensitive and confidential information). Note: some cloud services may not operate properly if you encrypt the data – be sure to understand whether encryption is available and how it impacts service standards with the vendor.

			YES	**NO**	**USER NOTES**
4	**Do you have a disaster recovery/business continuity plan?**				
a	Are backups stored in a safe, secure, and fireproof location?				
	i	Local backup?			
	ii	3rd party (cloud-based) backup provider?			
b	Can you recover your cloud data and/or cloud service from backup in the event of a data breach, the cloud provider loses your data or no longer provides cloud services to you?				
			YES	**NO**	**USER NOTES**
5	**Does your practice carry cyber risk insurance and liability insurance for ransomware attacks?**				
			YES	**NO**	**USER NOTES**
6	**In the event your data is locked or taken, do you know who you communicate to and how you would respond to clients and regulators?**				

This document is not intended to provide legal advice and is provided for informational use only.

Law Society of Saskatchewan Considerations

	Yes	No
1. Can you print (or convert to PDF) the following electronic records monthly?	□	□
a. trust journal	□	□
b. trust reconciliation including client trust listing	□	□
c. trust property record	□	□
2. Can electronic records be printed (or converted to PDF) on demand?	□	□
a. client trust ledger cards monthly	□	□
b. client trust at the conclusion of the matter	□	□
c. general journal	□	□
d. general bank reconciliation	□	□
e. billing journal	□	□
f. accounts receivable detail and listings	□	□
g. billings for all fees, charges and disbursements in chronological or numerical order	□	□
3. Do you maintain a hard copy or PDF of the master billings file?	□	□
4. Do you print or PDF all accounting records on an ongoing basis and store them appropriately?	□	□
5. Do your trust account reconciliations show the date that the reconciliation was completed?	□	□
a. Is an acceptable audit trail available on demand in a comprehensible format (print or PDF)?	□	□
6. Are all your cash receipts retained in hard copy form?	□	□
7. For all records, does the system record the creation and change dates?	□	□
a. Does the system preserve all metadata regarding electronic documents?	□	□
8. Have you considered your professional obligations that arise when you lose custody or control of your or your client's data?	□	□
9. Your electronic records must be capable of meeting the prevailing electronic discovery standards of the Courts. Have you verified this?	□	□

Checklist Completion

	Yes	No
1. Have you setup a re-occurring process that ensures your law practice reviews:	□	□
a. This document for revisions and changes?	□	□
b. For new regulatory acts that have been created?	□	□
c. Existing regulatory acts for changes in language?	□	□
d. Changes to the cloud services technology and/or how the cloud service is delivered which could affect security or regulation?	□	□
e. Cloud service providers agreements for compliance with regulations?	□	□
2. Have you fully completed this checklist and recorded the information for later reference?	□	□

This document is not intended to provide legal advice and is provided for informational use only.

Appendix A: Definitions

A glossary of terms related to cloud computing has been provided below. Not all of these terms have been used in the Guide and this is not an exhaustive list. By necessity, this Guide has focused on Canadian laws and regulations.

As practitioners engage with cloud service providers, they may encounter these concepts. As noted throughout the Guide, it is critical practitioners engage adequate technical expertise to vet any cloud service deployment to ensure a clear understanding of these concepts.

Term	Definition
Antivirus/Anti-malware	A type of utility used for scanning and removing viruses from your computer. While many types of antivirus (or "anti-virus") programs exist, their primary purpose is to protect computers from viruses and remove any viruses that are found.
Application Programming Interface (API)	A program that allows two applications to communicate with one another to access data. Every action you take on a smartphone, for example, such as sending direct messages or checking the weather, uses an API to access and deliver that information. APIs become critically important when you are looking at either (i) sharing internal firm information with a cloud service, or (ii) deploying multiple cloud services and ensuring that data from one service can be shared with data from another service.
Cloud Service Provider (CSP)	Companies that offer network services, infrastructure, or business applications in the cloud. The cloud services are hosted in a data center that can be accessed by companies or individuals using network connectivity.
Cloud Service	Any service made available to users on demand via the Internet from a CSP as opposed to being provided from a company's own on-premises servers. Cloud services are designed to provide easy, scalable access to applications, resources and services, and are fully managed by a CSP. A significant majority of the services used by individuals today are cloud services (e.g., Office 365, Uber, LinkedIn, Twitter, Zoom)
Data Centre	A central location for computer network hardware and software, especially storage devices for data. These are typically very large numbers of computers, physically located in close proximity in a very large facility and managed by a large incumbent technology company such as Amazon or Microsoft.
Encryption	A method of putting information in code so that only authorized users will be able to see or use the information.
GDPR	General Data Protection Regulation The General Data Protection Regulation is a European Union regulation on Information privacy in the European Union (EU) and the European Economic Area (EEA, and has three main purposes: • Harmonize the national data protection laws of all EU member states. • Ensure that organizations identify all personal data they handle from individuals in the EU and specify how it is

	protected, so that they can be fully transparent about their practices. • Grant customers new privacy rights and greater control over how their personal information is used by organizations.
Malware	Software programs designed to damage or do other unwanted actions on a computer system.
Multi-Tenant	A delivery model for Cloud Services where multiple users of the same software shares resources and access to those services. However, this does not typically mean that each user has access to the data of the other users. This can be contrasted with single tenant where the single user has a much higher degree of customization over the environment in which the Cloud Services are deployed.
Network	A group of computers that communicate with each other.
On-Premise	The deployment of software on hardware (computers) which is physically located on the user’s business premises. Prior to cloud, this is essentially how the majority of software was deployed (e.g., installing CD-ROM software on a server located at the Practitioner’s office(s)).
PIPEDA	The Personal Information Protection and Electronic Documents Act
Platform as a Service (PaaS)	A cloud computing model where a CSP delivers hardware (e.g., computers) and software tools (e.g., operating systems, databases) over the internet, typically so that the recipient (often a developer) can use those tools for application or database development.
Practitioner	A legal practitioner is a person who is authorized to practice law and provide legal services. This includes lawyers, paralegals, and other legal professionals who are regulated by the Law Society of Saskatchewan. Legal practitioners in Saskatchewan are bound by the rules of professional conduct and are responsible for providing competent, diligent, and ethical legal services to their clients.
Safe-harboured	Having a copy of your data stored securely by a 3rd provider separate from the cloud provider to guard against data loss and/or the cloud provider ceasing business.
Server	A computer that hosts systems or data for use by other computers on a network.
Service Level Agreement	The level of service you expect from a CSP, laying out the metrics by which service is measured, as well as remedies or penalties should the agreed-on service levels not be achieved.
Software as a Service (SaaS)	A method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers. Most Cloud Services offered today are deployed by this service method.
Virus	Computer viruses are small programs or scripts that can negatively affect the health of your computer.
Virtual Private Network (VPN)	Extends a private network across the internet and enables users to send and receive data as if their laptop or phone were directly connected to the cloud provider or service. The data is also encrypted during transmission over the network.