

Cloud computing checklist v. 4.0 [Updated January 2023]

Cloud computing offers many benefits to lawyers including the ability to access an array of new software services and applications, the offloading of hardware and software maintenance to cloud providers, the ability to access your data virtually and the reduction of large capital outlays. Since you are placing your data, and your clients' data, in the hands of third parties, it also raises issues of security and privacy, regulatory compliance and risk management, amongst others. This checklist is prepared with a view towards raising some of the issues that you should consider prior to moving data into the cloud. To better assist you with your risk management assessment, we erred on the side of inclusiveness while constructing this due diligence checklist. As legal professionals adjust to the cloud, we expect that the range of issues to consider may narrow. However, since cloud technologies continue to evolve, this checklist is drawn to include many issues.

Due diligence is not a one-and-done proposition, because new technologies develop, new opportunities arise, and new risks can manifest. Accordingly, our understanding of cloud computing is not static. Some matters in the checklist may be worth reviewing on a recurring basis or particularly if you consider large scale changes in how you practice. COVID-19 prompted legal professionals and others to embrace cloud technology in order to continue to operate. It remains important to understand how the technology can create benefits and risks, and also how developing law and policy may affect your legal and professional obligations.

One legal and policy development that lawyers should be aware of is the CLOUD Act.¹ The legislation is operative in the United States, and Canada and the United States are negotiating an agreement to make the legislation reciprocally enforceable in each jurisdiction. This checklist cannot function as a legal brief on the legislation or its current or future implications to a lawyer's practice or to the clients a law firm serves. But lawyers, particularly those who have clients whose activities may be of interest to the United States government or law enforcement, or who serve clients based in the United States whose activities may be of interest to either country's government or law enforcement agencies, are strongly encouraged to familiarize themselves with the legislation and remain abreast of how the negotiations for reciprocal enforcement of the CLOUD Act proceed.²

Lawyers requiring practice advice relating to these issues are encouraged to contact the Law Society's practice advisors. More general education is possible through continuing legal education materials on privacy and security, and academic research on the CLOUD Act.

While the Law Society does not provide a list of approved vendors, the Law Society may declare that a specific entity is not a permitted cloud storage provider (Rule 10-3(5)). You may wish to bring this to the attention of prospective vendors.

¹ *Clarifying Overseas Use of Lawful Data Act*, see, [Cloud Act Resources \(justice.gov\)](https://www.justice.gov/cloud-act-resources)

² A lawyer may also represent clients for whom the legislation creates a benefit, and it is important to understand this as well.

Introduction

- Are you contemplating a cloud product that is focused on the legal market – or one that is more general in design? *Comment: a cloud product designed for lawyers may have been developed with some professional, ethical and privacy requirements of lawyers in mind. However, it is up to you to perform your own due diligence. Do not simply rely on vendor marketing that says that a product or service is compliant with law society rules.*
- Is there a process that must be completed before anyone in your firm places your data on a cloud service? *Comment: having a process in place ensures that you perform your due diligence and consider the risks/benefits before moving any data to the cloud.*
- Consider that many records are your client’s property and information and that they have rights associated with these records. Your professional and legal obligations set out how you should deal with your client’s records.

Part A – First Steps	Yes	No
1. Read the cloud provider’s click-thru agreement.	<input type="checkbox"/>	<input type="checkbox"/>
2. Review the cloud provider's SLA (service level agreement). ³	<input type="checkbox"/>	<input type="checkbox"/>
3. Review the cloud provider's privacy and confidentiality agreement. ⁴	<input type="checkbox"/>	<input type="checkbox"/>

³ The foundation of adequate due diligence is understanding the terms and conditions of the service you are using.

⁴ The foundation of adequate due diligence is understanding the terms and conditions of the service you are using.

Part B – Law Society of British Columbia Considerations ⁵	Yes	No
1. Are the electronic records capable of meeting the auditing and investigation standards for accounting records and client identification and verification records required by the Law Society? ⁶	<input type="checkbox"/>	<input type="checkbox"/>
a. Can electronic records be printed in a comprehensive format, accessed on a read-only basis, and exported to an electronic format that allows access to the records in a comprehensive format? (Rule 10-3)	<input type="checkbox"/>	<input type="checkbox"/>
b. Are electronic records available on demand and in a format acceptable to the Law Society? (Rule 10-3)	<input type="checkbox"/>	<input type="checkbox"/>
c. Can the metadata regarding the electronic records be made available to the Law Society on demand? (A “record” includes “metadata” associated with an electronic record (Rule 1))	<input type="checkbox"/>	<input type="checkbox"/>
d. Do you print or PDF a full and complete client trust ledger at the close of each client matter?	<input type="checkbox"/>	<input type="checkbox"/>
e. Are print or PDF bank reconciliations (for all trust and general bank accounts) created the same day they are completed and stored?	<input type="checkbox"/>	<input type="checkbox"/>
f. Is a master billings file always maintained in hard copy or PDF?	<input type="checkbox"/>	<input type="checkbox"/>
g. Do you print or PDF all accounting records required by Division 7 Part 3 of the Law Society Rules on an ongoing basis (and store them appropriately)?	<input type="checkbox"/>	<input type="checkbox"/>
2. Do your trust account reconciliations show the date that the reconciliation was completed?	<input type="checkbox"/>	<input type="checkbox"/>
a. With appropriate background information?	<input type="checkbox"/>	<input type="checkbox"/>
i. Is all background information imaged (front and back including blank pages)?	<input type="checkbox"/>	<input type="checkbox"/>
b. Is the data of the reconciliation incapable of being overwritten?	<input type="checkbox"/>	<input type="checkbox"/>
c. Do billing records record the creation and all modification dates?	<input type="checkbox"/>	<input type="checkbox"/>
d. Is an audit trail available (and printable) on demand in a comprehensible format?	<input type="checkbox"/>	<input type="checkbox"/>
i. Is the audit trail complete showing all postings in the software?	<input type="checkbox"/>	<input type="checkbox"/>
ii. Do transactions correspond with specifically assigned transactions corresponding with dates?	<input type="checkbox"/>	<input type="checkbox"/>
3. Are cash receipts maintained and retained in hard copy form? (Rule 3-70, 3-75)	<input type="checkbox"/>	<input type="checkbox"/>

⁵ It is essential that lawyers can comply with the Law Society requirements when using third party service providers to store and process data. While later parts of the checklist that are designed to help lawyers understand some of the business risks may have variable significance to lawyers depending on the nature of their practice, the necessity of complying with Law Society requirements applies to all lawyers.

⁶ See Law Society Rules 3-60(2), 3-67 to 3-73, 3-75 to 3-76, 3-85 to 3-86, 3-107, 4-55, and 10-3 to 10-4. Rule 10-3(2) requires that, when required under the *Legal Profession Act* or the rules, a lawyer must, on demand, promptly produce records in any or all of the following forms: (a) printed in a comprehensive format; (b) accessed on a read-only basis; (c) exported to an electronic format that allows access to the records in a comprehensible format.

4. For all records, does the system record the creation date, edits and the dates that such edits were made?	<input type="checkbox"/>	<input type="checkbox"/>
a. Does the system preserve all metadata regarding electronic documents?	<input type="checkbox"/>	<input type="checkbox"/>
5. When the Law Society copies your electronic records, it can rely on the copies as “best evidence.”	<input type="checkbox"/>	<input type="checkbox"/>
a. Where a member disputes the quality of the electronic records of the lawyer, the onus is on the lawyer to provide a forensic copy of these records at the lawyer's expense.		
6. Can the Law Society obtain, view and print access to all records when required?	<input type="checkbox"/>	<input type="checkbox"/>
7. Will the cloud provider assist you to comply with your professional obligations related to the records?	<input type="checkbox"/>	<input type="checkbox"/>
a. Including compliance with the Law Society’s regulatory process	<input type="checkbox"/>	<input type="checkbox"/>
8. Does the cloud provider archive data for periods that meet or exceed the Law Society’s retention requirements? See Rules 3-55, 3-73(4), 3-75(2), 3-107. Are you able to delete records maintained with a service provider when required by law to do so?	<input type="checkbox"/>	<input type="checkbox"/>
a. Are electronic records retained for a minimum of 10 years from the final accounting transaction?	<input type="checkbox"/>	<input type="checkbox"/>
9. What is the dispute resolution method in the cloud provider’s SLA? _____ _____		
a. What is the governing law for the SLA? _____ _____		
10. Consider your professional obligations that arise when you lose custody or control of your records including ensuring that a written report is provided to the Executive Director (e.g. Law Society Rule 10-4(2)) and reporting to the Lawyers Indemnity Fund (Rule 3-39 and BC Code section 7.8)	<input type="checkbox"/>	<input type="checkbox"/>
11. If you are the victim of a data breach immediately report your claim to your cyber insurer .	<input type="checkbox"/>	<input type="checkbox"/>
12. Read Law Society Rules 10-3 and 10-4. Can you meet the requirements of these rules while using the cloud service?		
13. Do you have a plan in place to allow the Law Society access to passwords to retrieve documents should it be required (e.g. the Law Society acting as custodian)?	<input type="checkbox"/>	<input type="checkbox"/>

Part C – Security and Risk Management	Yes	No
1. Have specific risks been identified when using this particular cloud provider/application? <i>Comment: Doing an internet search for user reviews of a particular cloud application may reveal difficulties and issues with this provider or application that should be considered.</i>	<input type="checkbox"/>	<input type="checkbox"/>
2. Has the cloud provider had any security breaches?	<input type="checkbox"/>	<input type="checkbox"/>
a. Are you satisfied with the cloud provider’s response to any security breaches that they may have had?	<input type="checkbox"/>	<input type="checkbox"/>
3. Are you satisfied the cloud provider has adequate technological, contractual, and policy safeguards in place to ensure data that may be confidential and/or subject to solicitor-client privilege is properly protected?	<input type="checkbox"/>	<input type="checkbox"/>
a. Is your data aggregated and de-identified ⁷ ?	<input type="checkbox"/>	<input type="checkbox"/>
4. Is your data safe-harboured? <i>Comment: “Safe-harboured” means 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.</i>	<input type="checkbox"/>	<input type="checkbox"/>
5. Have you considered a private cloud vs. a public cloud? <i>Comment: The term “private cloud” is meant to describe a cloud computing platform that is implemented internally within your corporate firewall, under the control of your IT department. A private cloud is designed to offer the features and benefits of public cloud systems, but a private cloud removes some concerns, particularly around external control over enterprise and customer data and regulatory compliance.</i>	<input type="checkbox"/>	<input type="checkbox"/>

⁷ According to the Office of the Privacy Commissioner of Canada: “Private sector companies may aggregate personal information about their customers for internal purposes and analysis and some companies may sell their aggregated data for profit. Other companies’ business models are founded on combining various sets of aggregated data with sets of publicly available information to produce valuable data sets that help companies make predictions about customers and better target customers or engage in “data mining” practices. When data is aggregated, organizations often claim that they anonymize data such that it no longer fits within the definition of “personal information” under PIPEDA.

However, several researchers have recently shown that de-identified data is often not very anonymous and pieces of data can easily be re-identified or “reattached” to information about an identifiable person. This practice of re-identification is problematic because oftentimes consumers do not realize that the commercial bartering of their personal information is a burgeoning and profitable industry.

As organizations collect an increasing amount of personal information about consumers, their practices of de-identifying this personal information should be scrutinized to ensure that the data has been de-identified to a sufficient degree to protect the consumer from re-identification and potential harms that could flow from the use of de-identified data. Industry best practices regarding de-identification and anonymization would serve to bring increased transparency to garner consumer trust in personal information practices.

De-identified data and the questions around re-identification are growth industries. Given the potential harms to consumers and citizens, the OPC must monitor this question closely and provide timely guidance to industry - and comfort to consumers - to assure all parties they are aware of how individuals are or may become identifiable in the course of regular commercial data processing.” [http://www.priv.gc.ca/resource/cp/2010-2011/p_201011_09_e.asp] [Note: this is now an archived record of the Privacy Commissioner’s Office.]

<p>6. Are you considering moving a mission critical system to the cloud? <i>Comment: A mission critical system is one whose failure or loss would severely jeopardize your ability to remain in business or meet your professional obligations.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>7. If your data is not stored in encrypted form, can you use an encryption product to protect your data? <i>Comment: Some cloud services may not be able to operate properly if you encrypt your data. Others are fine with encryption.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>8. Can you maintain a local backup of your data? a. What can you do with your data backup if the cloud provider disappears for whatever reason or alters the terms of service (e.g. a dramatic increase in cost of service to maintain access to your records) in a manner that leaves you little time to migrate your files off of their system? <i>Comment: Many cloud providers use a proprietary application or system to organize and manipulate your data. Having a copy of your data may not be all that useful if you are unable to export it into another product and regain all the relationships between the data.</i></p> <p>_____</p> <p>_____</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>9. Who is responsible within your firm for the security of your data? Does the cloud provider have a contact for trouble-shooting? <i>Comment: There are at least four components to data security: 1. Firewall, 2. Encryption, 3. Password Protection and 4. Physical Security (locked doors and such). Any data security plan should address all four.</i></p> <p>_____</p> <p>_____</p>		
<p>10. Are your remedies adequate in the event of data breaches, indemnification obligations, and service availability failure?</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>11. Do you have an accessible master list of your clients contact information in the event you need to notify them of a data breach?</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>12. Who within your firm is responsible for privacy and regulatory compliance?</p> <p>_____</p> <p>_____</p>		
<p>13. What ability do you have to audit or view audits of the cloud provider's performance? <i>Comment: 3rd party verification of a cloud provider's security implementation should be one of the aspects to establishing trust in a cloud provider. Do they produce audit reports on a regular basis that are conducted by reputable 3rd party experts?</i></p> <p>_____</p> <p>_____</p>		
<p>a. How often does the cloud provider have their security audited?</p> <p>_____</p>		

14. If the cloud provider ceases business, how long will it take you to get your data and convert to another provider (if at all)? <i>Comment: Investigating in advance if there is any alternative to a cloud provider that can import your data and maintain the usefulness of the data after the conversion is a good risk management step.</i> _____		
a. What format will your data be in? _____		
15. Does the cloud provider use cloud services itself (clouds of clouds)?	<input type="checkbox"/>	<input type="checkbox"/>
a. Is the cloud provider required to give notice if contemplating contracting out to other providers? (known as “clouds of clouds”) <i>Comment: If a cloud provider itself contracts out to another cloud provider, it may jeopardize your desire to keep all your data within Canada, for example.</i>	<input type="checkbox"/>	<input type="checkbox"/>
16. Is the cloud provider responsible for sub-contractors?	<input type="checkbox"/>	<input type="checkbox"/>
17. Do you have a disaster recovery/business continuity plan? ⁸	<input type="checkbox"/>	<input type="checkbox"/>
a. Have you stored your backups and key information in preparation for a fire, flood, earthquake or other disaster?	<input type="checkbox"/>	<input type="checkbox"/>
18. Is the cloud provider required to indemnify you for losses as a result of using their service?	<input type="checkbox"/>	<input type="checkbox"/>
a. Have you made inquiries as to third-party insurance to cover this?	<input type="checkbox"/>	<input type="checkbox"/>

⁸ See, Law Society of British Columbia’s practice resources, “What to do Before and After a Disaster Strikes” at [Practice Resource - What to do Before and After a Disaster Strikes \(lawsociety.bc.ca\)](http://lawsociety.bc.ca).

Part D - Compliance⁹	Yes	No
1. Do you have a firm privacy policy and is the contemplated cloud service consistent with your privacy policy?	<input type="checkbox"/>	<input type="checkbox"/>
2. Where are the cloud provider's servers located? _____		
a. Do they have multiple storage locations?	<input type="checkbox"/>	<input type="checkbox"/>
b. Who has access to your data? _____		
c. What are the guarantees or representations from the cloud provider regarding the security of your data? _____ _____		
d. What laws are applicable to your data? (local, federal jurisdictional issues; consider here, also international laws like The CLOUD Act and related enforcement treaties) _____ _____ <i>Comment: Identify the privacy legislation and other applicable legislation regulating the protection and disclosure of your client's data.¹⁰</i>		
3. Your electronic records must be capable of meeting the prevailing electronic discovery standards of the BC Superior Courts. Have you verified this?	<input type="checkbox"/>	<input type="checkbox"/>
4. How sensitive is your data? _____		
a. Are there any specific laws that restrict placing your client's data in the cloud?	<input type="checkbox"/>	<input type="checkbox"/>
i. Outside of BC?	<input type="checkbox"/>	<input type="checkbox"/>
ii. Outside of Canada? ¹¹	<input type="checkbox"/>	<input type="checkbox"/>
iii. What substantive and procedural laws apply to your data? _____ _____		
b. You must comply with all privacy legislation applicable to the data under consideration:	<input type="checkbox"/>	<input type="checkbox"/>

⁹ In addition to regulatory compliance with the Law Society, lawyers need to ensure they comply with other laws that affect their collection, use and retention of data / personal information.

¹⁰ See, Office of the Information and Privacy Commissioner for British Columbia, "Reasonable security measures for personal information disclosures outside of Canada" (March 2022) at [3646 \(oipc.bc.ca\)](https://oipc.bc.ca).

¹¹ For example, if you have clients who are living in the European Union and your services are subject to the *General Data Protection Regulation 2016/679*, you must ensure you are complying with its requirements; see <https://gdpr-info.eu/>.

<p>i. <i>BC's Personal Information Protection Act, SBC 2003 c. 63 (PIPA)</i></p> <p>ii. <i>Federal Personal Information Protection and Electronic Documents Act, SC 2000 c 5 (PIPEDA)</i></p> <p>iii. <i>Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 (FIPPA)</i></p> <p><i>Comment: If applicable, see BC Reg 294/2021 Personal Information Disclosure for Storage Outside of Canada Regulation CanLII.</i></p>		
<p>c. Private sector</p>		
<p>i. Lawyer must enter into a data protection arrangement with the cloud provider that ensures equivalent levels of data protection as are required by BC/Canada</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>ii. Consent is required from the client if personal information is being disclosed for a secondary purpose (consider the risk for confidential and privileged information).</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>iii. The openness principle as incorporated into the Cloud Computing Report by the Law Society makes it a best practice to provide notice to the client that data will be processed and/or stored outside Canada, if applicable.</p> <p>This might include whether a foreign state has the authority to access the data for lawful access purposes.</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>iv. Lawyer's policy and practices must indicate:</p>		
<ul style="list-style-type: none"> • Countries outside Canada where the collection, use and disclosure will occur. 	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • The purpose(s) for which the cloud provider has been authorized to collect, use or disclose personal information. 	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • Before or at the time of collecting or transferring personal information to a cloud provider outside of Canada, the lawyer must notify the client of: 		
<ul style="list-style-type: none"> - The way to obtain access to written information about the lawyer's policies and practices regarding service providers outside of Canada. 	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> - The name or position of a person who is able to answer the individual's questions about the collection, use, disclosure or storage of personal information by the service providers outside of Canada. 	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • While the notification may not require information about countries outside of Canada (this is a best practice in the Law Society's Cloud Computing Report), the lawyer's privacy policy should contain this information. 	<input type="checkbox"/>	<input type="checkbox"/>
<p>d. What encryption method is applicable to the data?</p> <p><i>Manage Encryption.</i></p> <ul style="list-style-type: none"> • <i>Understand what type of encryption method is used.</i> • <i>Identify where data is encrypted or unencrypted at each stage (e.g., data in-transit, data at-rest).</i> • <i>Conduct an assessment of risks associated with any lack of encryption. Determine if encryption the method is adequate and if access to the encryption key is properly managed. In terms of maintaining confidentiality, it is better if the lawyer or law firm is the sole owner of the encryption key rather than a public cloud provider.</i> • <i>Risks may be reduced if personal information is encrypted before it is sent to the cloud provider. Although encryption at rest and in-transit are the gold standard, some commonly used legal software application providers may have reasons why they</i> 		

<i>do not encrypt data at-rest. Discuss this with your provider and make an informed decision.</i>		
i. In transmission? <i>Data in-transmission means data is encrypted while it travels from where you are inputting it to the cloud-based server.</i>	<input type="checkbox"/>	<input type="checkbox"/>
ii. In storage? <i>Data in storage means data is encrypted while it is stored on the cloud-based server.</i>	<input type="checkbox"/>	<input type="checkbox"/>
e. Can the cloud provider access your data or metadata?	<input type="checkbox"/>	<input type="checkbox"/>
i. If so, for what purpose(s)? _____ _____		
f. Is the confidentiality and privilege of your client's information reasonably protected? <i>Comment: Consider, amongst other things, the answer to questions d and e above.</i>	<input type="checkbox"/>	<input type="checkbox"/>
g. Have you considered establishing a private cloud for sensitive data or data that cannot leave the jurisdiction?	<input type="checkbox"/>	<input type="checkbox"/>
5. What are the cloud provider's breach notification requirements? _____	<input type="checkbox"/>	<input type="checkbox"/>

Part E – (Further) Due Diligence	Yes	No
1. What are your roles and responsibilities (vs. the cloud provider's responsibilities) after you have moved to using a cloud provider? _____ _____		
2. Can you terminate the service?	<input type="checkbox"/>	<input type="checkbox"/>
a. At what cost or penalty or on what terms? _____ _____		
b. What if a security or privacy breach occurs? <i>Comment: You may have further issues to consider if a privacy or security breach occurs, such as notice to the client, notice to the Law Society (Rule 10-4), notice to your insurer(s) and the like.</i> _____ _____		
c. What if performance, bandwidth or reliability promises are not being met? _____ _____		

d. What if material modifications are made to the cloud service terms? ¹² _____		
e. Is your data available after termination?	<input type="checkbox"/>	<input type="checkbox"/>
i. For how long? _____		
ii. In what format? _____		
f. Is the cloud provider required to provide transition support if the service is terminated?	<input type="checkbox"/>	<input type="checkbox"/>
g. Can your data be sanitized from the cloud provider in the event of a termination? <i>Comment: sanitized in this context would mean removing all trace of the lawyer's data from the cloud provider's service.</i>	<input type="checkbox"/>	<input type="checkbox"/>
h. Does the SLA transfer intellectual property rights and/or ownership rights in your data? <i>Comment: Rule 10-3(4) requires a lawyer to ensure that ownership of the lawyer's records do not pass to another party.</i>	<input type="checkbox"/>	<input type="checkbox"/>
3. Have you compared the cloud product against alternative (non-cloud) applications?	<input type="checkbox"/>	<input type="checkbox"/>
a. What are the advantages or disadvantages of each? _____		
4. What notice needs to be given and how is that notice given when the SLA agreement and other underlying policies are changed? _____		
5. Is there a cap on the cloud provider's liability?	<input type="checkbox"/>	<input type="checkbox"/>
6. What happens if the cloud provider ceases business or has their servers seized or destroyed? _____		
7. Do you have access to the cloud provider's source code (via an escrow agreement or otherwise) if they cease to do business? <i>Comment: Without the source code or alternatively, the ability to move your data to another provider, your data may be largely unusable and you may be facing other risks as a result, such as the inability to maintain the systems necessary to stay in practice.</i>	<input type="checkbox"/>	<input type="checkbox"/>
8. Do you regularly review the cloud provider with a view to whether or not changes in the cloud provider's use of technology might affect their acceptability for use by a BC lawyer?	<input type="checkbox"/>	<input type="checkbox"/>
9. Does the cloud provider put you off-side a legal obligation? <i>Comment: If so, don't use the service.</i>	<input type="checkbox"/>	<input type="checkbox"/>
10. Have you considered whether it is possible to establish a records-management system that would aggregate all cloud and non-cloud based records by client file in a secure location?	<input type="checkbox"/>	<input type="checkbox"/>

¹² Consider the value of periodically reviewing existing services to ensure material changes have not put you off-side regulatory or legal requirements.

11. Have you documented your due diligence and kept a copy of the information for later reference?

Part F– Client Implications	Yes	No
1. The Law Society’s Cloud Computing Report has set out that it is a best practice to receive the informed consent from your client to store their data in the cloud. Have you considered securing this consent from your client (in writing) by placing this in your retainer agreement? Have you informed existing clients of the move to a cloud based service to get their consent to storage outside Canada, where applicable? Ensure you comply with the applicable privacy legislation.	<input type="checkbox"/>	<input type="checkbox"/>
2. Does your client have concerns about personal information being stored in the cloud?	<input type="checkbox"/>	<input type="checkbox"/>
Part G – IT Considerations		
1. Does the cloud application integrate with your other office systems?	<input type="checkbox"/>	<input type="checkbox"/>
2. Are there workflow advantages to moving to the cloud?	<input type="checkbox"/>	<input type="checkbox"/>
3. Is the system available 24/7?	<input type="checkbox"/>	<input type="checkbox"/>
a. Is this an extra cost?	<input type="checkbox"/>	<input type="checkbox"/>
4. Do you have sufficient bandwidth to run the cloud application with acceptable performance? <i>Comment: Bandwidth is determined by your data contract with your internet service provider (“ISP”). You may have to obtain greater capacity, a faster connection or both [at greater cost] to obtain acceptable performance at peak load times. You may wish to raise this with your ISP.</i>	<input type="checkbox"/>	<input type="checkbox"/>
a. Have you tested the system while running all other systems? <i>Comment: Do a test with dummy data before committing to the system.</i>	<input type="checkbox"/>	<input type="checkbox"/>
b. What is the maximum bandwidth that you can access?		
5. Can the system handle demands for increased capacity or spikes due to rapid growth?	<input type="checkbox"/>	<input type="checkbox"/>
a. Can you reduce capacity (at what cost) if your needs diminish?	<input type="checkbox"/>	<input type="checkbox"/>
6. Does the provider have at least three types of security?		
a. Company-based security (intrusion detection and prevention, spam and virus filters etc.)	<input type="checkbox"/>	<input type="checkbox"/>
b. Access based security (based on identity or role of an individual in your organization)	<input type="checkbox"/>	<input type="checkbox"/>
c. Transport-based security (such as Virtual Private Network or VPN, Secure Socket Layer or SSL tunneling or encryption)	<input type="checkbox"/>	<input type="checkbox"/>
7. Help Desk Hours		
a. Do the times match your typical operating hours?	<input type="checkbox"/>	<input type="checkbox"/>
b. What about emergency contact information? 24/7?	<input type="checkbox"/>	<input type="checkbox"/>
c. What kind(s) of support is provided? i. Phone hotline/email/web-based chat?	<input type="checkbox"/>	<input type="checkbox"/>
d. Is there an extensive knowledge base on the cloud service?	<input type="checkbox"/>	<input type="checkbox"/>
8. What are the backup systems of the cloud provider?		
a. Where are they located?	<input type="checkbox"/>	<input type="checkbox"/>

b. Does this cause difficulties with regard to location of data requirements?	<input type="checkbox"/>	<input type="checkbox"/>
c. Is the cloud provider required to notify you if they change backup providers?	<input type="checkbox"/>	<input type="checkbox"/>
d. How often do they backup their data? _____		
e. Do they have redundant or fail-over systems, such as RAID? <i>Comment: RAID stands for "Redundant Array of Inexpensive (or Independent) Discs" and is a method to ensure that data is written into many disks to guard against disk – and data loss.</i>	<input type="checkbox"/>	<input type="checkbox"/>
9. In the event of a disaster, can you achieve acceptable recovery point objectives (RPOs) and recovery time objectives (RTOs)?	<input type="checkbox"/>	<input type="checkbox"/>
10. In what format is your data stored? _____		
11. Is your IT support comfortable supporting a hybrid environment (part cloud, part not)?	<input type="checkbox"/>	<input type="checkbox"/>

Part H – Reliability		
1. What is the cloud provider's "up" history? <i>Comment: "Up" time is the time the cloud provider's services are available for use. The most desired or gold standard is 99.999% of the time.</i>		
a. How do they calculate up-time? _____ _____		
2. If the cloud provider has gone down, what was the longest time period they were down? _____		
a. What are your costs or lost-revenue per hour if the service becomes unavailable? _____		
3. Can you operate offline if the system goes down?	<input type="checkbox"/>	<input type="checkbox"/>
4. Are availability, performance and bandwidth representations spelled out in the SLA?	<input type="checkbox"/>	<input type="checkbox"/>
a. What, if any, are the penalties for failing to meet these? _____ _____		
5. What reports will be delivered regarding system reliability? _____ _____		
6. What notice will be given for maintenance periods? _____		
a. Are the cloud provider's schedule for maintenance acceptable?	<input type="checkbox"/>	<input type="checkbox"/>

Part I – Fees & Cost	Yes	No
1. What is your initial set-up fee? _____		
2. What are your monthly (ongoing) fees? _____		
3. Are there usage or bandwidth fees?	<input type="checkbox"/>	<input type="checkbox"/>
4. Does using this product increase your in-office costs?	<input type="checkbox"/>	<input type="checkbox"/>
5. How often (and by how much) can the provider increase fees? _____		
a. Is there a cap on price increases?	<input type="checkbox"/>	<input type="checkbox"/>
6. What are your total internal costs (hardware, software and soft-costs) in converting to this cloud service? _____		
a. Do you have any anticipated cost-savings?	<input type="checkbox"/>	<input type="checkbox"/>
7. Have you compared the cost of the cloud service vs. non-cloud alternatives (present value calculation)?	<input type="checkbox"/>	<input type="checkbox"/>
8. Can the cloud provider cut off your access to your data in the event of non-payment of fees or for other reason(s)?	<input type="checkbox"/>	<input type="checkbox"/>

If you have any practice advice questions relating to using cloud computing, please contact a practice advisor at practiceadvice@lsbc.org.

If you have any recommendations for improving or updating the policies reflected in this checklist, please contact Doug Munro at dmunro@lsbc.org.