The Law Society of British Columbia

Practice Resource

Cloud computing checklist v. 3.0 [Updated April 2020]

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 and upkeep to cloud providers, the ability to access your data from virtually everywhere 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 has been prepared with a view towards raising some of the issues that should be considered prior to a lawyer or law firm 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 lawyers and law firms adjust to the cloud, it is expected that the range of issues to be considered will narrow. However, since the cloud is still relatively new to lawyers and law firms, this checklist has been drawn to be inclusive of as many of the issues as possible.

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)). Lawyers may wish to bring this to the attention of prospective vendors.

Introduction

- "As with most things IT these days, you need to think like a lawyer when moving to the cloud." (from HP Communities)

- 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 the professional, ethical and privacy requirements of lawyers in mind.*

- 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 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.	☐	☐
2. Review the cloud provider's SLA (Service Level Agreement).[1]	☐	☐
3. Review the cloud provider's Privacy and Confidentiality Agreement.[2]	☐	☐

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

[2] See note 1.

Part B – Law Society of British Columbia Considerations[3]	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?[4]	☐	☐
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)	☐	☐
b. Are electronic records available on demand and in a format acceptable to the Law Society? (Rule 10-3)	☐	☐
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).)	☐	☐
d. Do you print or PDF a full and complete client trust ledger at the close of each client matter?	☐	☐
e. Are print or PDF bank reconciliations (for all trust and general bank accounts) created the same day they are completed and stored?	☐	☐
f. Is a master billings file always maintained in hard copy or PDF?	☐	☐
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)?	☐	☐
2. Do your trust account reconciliations show the date that the reconciliation was completed?	☐	☐
a. With appropriate background information?	☐	☐
i. Is all background information imaged (front and back including blank pages)?	☐	☐
b. Is the data of the reconciliation incapable of being overwritten?	☐	☐
c. Do billing records record the creation and all modification dates?	☐	☐
d. Is an audit trail available (and printable) on demand in a comprehensible format?	☐	☐
i. Is the audit trail complete showing all postings in the software?	☐	☐
ii. Do transactions correspond with specifically assigned transactions corresponding with dates?.	☐	☐
3. Are cash receipts maintained and retained in hard copy form? (Rule 3-70, 3-75)	☐	☐

[3] 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.

[4] 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. 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?	☐	☐
a. Does the system preserve all metadata regarding electronic documents?	☐	☐
5. When the Law Society copies your electronic records, it can rely on the copies as "best evidence".	☐	☐
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?	☐	☐
7. Will the cloud provider assist you in complying with your professional obligations related to the records?	☐	☐
a. Including compliance with the Law Society's regulatory process	☐	☐
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.	☐	☐
a. Are electronic records retained for a minimum of 10 years from the final accounting transaction?	☐	☐
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 Rule10-4(2)).	☐	☐
11. Read Law Society Rules 10-3 and 10-4. Can you meet the requirements of these rules while using the cloud service?	☐	☐
12. 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).	☐	☐

Part C – Security and Risk Management	Yes	No
4. Have specific risks been identified when using this particular cloud provider/application? *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.*	☐	☐
5. Has the cloud provider had any security breaches?	☐	☐
a. Are you satisfied with the cloud provider's response to any security breaches that they may have had?	☐	☐
6. 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?	☐	☐
a. Is your data aggregated and de-identified[5]?	☐	☐
7. Is your data 'safe-harboured'? *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.*	☐	☐
8. Have you considered a 'private cloud' vs. a 'public cloud'? *Comment: Webopedia states: The phrase 'private cloud' is used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of public cloud systems, but [a private cloud] removes a number of objections to the cloud computing model including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.*	☐	☐
9. Are you considering moving a 'mission critical' system to the cloud?	☐	☐

[5] 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]

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.		
10. If your data is not stored in encrypted form, can you use an encryption product to protect your data? *Comment: Some cloud services may not be able to operate properly if you encrypt your data. Others are fine with encryption.*	☐	☐
11. 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? *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.* _____ _____		
12. Who is responsible within your firm for the security of your data? Does the cloud provider have a contact for trouble-shooting? *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.* _____ _____		
13. Are your remedies adequate in the event of: data breaches, indemnification obligations, and service availability failure?	☐	☐
14. Do you have an accessible master list of your clients contact information in the event you need to notify them of a data breach?	☐	☐
15. Who within your firm is responsible for privacy and regulatory compliance? _____ _____		
16. What ability do you have to audit or view audits of the cloud provider's performance? *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?* _____ _____		
a. How often does the cloud provider have their security audited? _____		
17. If the cloud provider ceases business, how long will it take you to get your data and convert to another provider (if at all)?		

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. _____		
a. What format will your data be in? _____		
18. Does the cloud provider use cloud services itself ('clouds of clouds')?	☐	☐
a. Is the cloud provider required to give notice if contemplating contracting out to other providers? (known as 'clouds of clouds') *Comment: having a cloud provider itself contract out to another cloud provider may jeopardize your desire to keep all your data within Canada, for example.*	☐	☐
19. Is the cloud provider responsible for sub-contractors?	☐	☐
20. Do you have a disaster recovery/business continuity plan?	☐	☐
a. Are backups stored in a safe, secure and fireproof location?	☐	☐
21. Is the cloud provider required to indemnify you for losses as a result of using their service?	☐	☐
a. Have you made inquiries as to third-party insurance to cover this?	☐	☐

Part D - Compliance[6]	Yes	No
1. Do you have a firm privacy policy and is the contemplated cloud service consistent with your privacy policy?	☐	☐
2. Where are the cloud provider's servers located? _____		
a. Do they have multiple storage locations?	☐	☐
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) _____ _____ *Comment: Identify the privacy legislation and other applicable legislation regulating the protection and disclosure of your client's data.*		
3. Your electronic records must be capable of meeting the prevailing electronic discovery standards of the BC Superior Courts. Have you verified this?	☐	☐
4. How sensitive is your data? _____		
a. Are there any specific laws that restrict placing your client's data in the cloud?	☐	☐
i. Outside of BC?	☐	☐
ii. Outside of Canada?[7]	☐	☐
iii. What substantive and procedural laws apply to your data? _____ _____		
b. You must comply with all privacy legislation applicable to the data under consideration: i. *BC's Personal Information Protection Act*, SBC 2003 c. 63 (PIPA) ii. *Federal Personal Information Protection and Electronic Documents Act*, SC 2000 c 5 (PIPEDA) iii. *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 (FIPPA) *Comment: if applicable, you must ensure that all data is stored or accessed only within Canada (unless one of the exceptions is met).*	☐	☐

[6] 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.

[7] 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/.

c. Private sector		
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	☐	☐
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).	☐	☐
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. This might include whether a foreign state has the authority to access the data for lawful access purposes.	☐	☐
iv. Lawyer's policy and practices must indicate:		
• Countries outside Canada where the collection, use and disclosure will occur.	☐	☐
• The purpose(s) for which the cloud provider has been authorized to collect, use or disclose personal information.	☐	☐
• 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:		
- The way to obtain access to written information about the lawyer's policies and practices regarding service providers outside of Canada.	☐	☐
- 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.	☐	☐
• 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.	☐	☐
d. What encryption method is applicable to the data? *Manage Encryption.* • *Understand what type of encryption method is used.* • *Identify where data is encrypted or unencrypted at each stage (e.g., data in-transit, data at-rest).* • *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.* • *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 do not encrypt data at-rest. Discuss this with your provider and make an informed decision.*		
i. In transmission? *Data in-transmission means data is encrypted while it travels from where you are inputting it to the cloud-based server.*	☐	☐
ii. In storage? *Data in storage means data is encrypted while it is stored on the cloud-based server.*	☐	☐

e. Can the cloud provider access your data or metadata?	☐	☐
i. If so, for what purpose(s)? _____ _____		
f. Is the confidentiality and privilege of your client's information reasonably protected? *Comment: consider, amongst other things, the answer to questions d and e above.*	☐	☐
g. Have you considered establishing a private cloud for sensitive data or data that cannot leave the jurisdiction?	☐	☐
5. What are the cloud provider's breach notification requirements? _____	☐	☐

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?	☐	☐
a. At what cost or penalty or on what terms? _____ _____		
b. What if a security or privacy breach occurs? *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.* _____ _____		
c. What if performance, bandwidth or reliability promises are not being met? _____ _____		
d. What if material modifications are made to the cloud service terms?[8] _____ _____		
e. Is your data available after termination?	☐	☐
i. For how long? _____		
ii. In what format? _____		

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

f. Is the cloud provider required to provide transition support if the service is terminated?	☐	☐
g. Can your data be sanitized from the cloud provider in the event of a termination? *Comment: sanitized in this context would mean removing all trace of the lawyer's data from the cloud provider's service.*	☐	☐
h. Does the SLA transfer intellectual property rights and/or ownership rights in your data? *Comment: Rule 10-3(4) requires a lawyer to ensure that ownership of the lawyer's records do not pass to another party.*	☐	☐
3. Have you compared the cloud product against alternative (non-cloud) applications?	☐	☐
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?	☐	☐
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? *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.*	☐	☐
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?	☐	☐
9. Does the cloud provider put you off-side a legal obligation? *Comment: if so, don't use the service.*	☐	☐
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?	☐	☐
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.	☐	☐
2. Does your client have concerns about personal information being stored in the cloud?	☐	☐
Part G – IT Considerations		
1. Does the cloud application integrate with your other office systems?	☐	☐
2. Are there workflow advantages to moving to the cloud?	☐	☐
3. Is the system available 24/7?	☐	☐
a. Is this an extra cost?	☐	☐
4. Do you have sufficient bandwidth to run the cloud application with acceptable performance? *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).*	☐	☐
a. Have you tested the system while running all other systems? *Comment: do a test with dummy data before committing to the system.*	☐	☐
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?	☐	☐
a. Can you reduce capacity (at what cost) if your needs diminish?	☐	☐
6. Does the provider have at least three 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)	☐	☐
7. Help Desk Hours		
a. Do the times match your typical operating hours?	☐	☐
b. What about emergency contact information? 24/7?	☐	☐
c. What kind(s) of support is provided? i. Phone hotline/email/web-based chat?	☐	☐
d. Is there an extensive knowledge base on the cloud service?	☐	☐
8. What are the backup systems of the cloud provider?		
a. Where are they located?	☐	☐

b. Does this cause difficulties with regard to location of data requirements?	☐	☐
c. Is the cloud provider required to notify you if they change backup providers?	☐	☐
d. How often do they backup their data? _____		
e. Do they have redundant or fail-over systems, such as RAID? *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.*	☐	☐
9. In the event of a disaster, can you achieve acceptable recovery point objectives (RPOs) and recovery time objectives (RTOs)?	☐	☐
10. In what format is your data stored? _____		
11. Is your IT support comfortable supporting a hybrid environment (part cloud, part not)?	☐	☐

Part H – Reliability		
1. What is the cloud providers "up" history? *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.*		
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?	☐	☐
4. Are availability, performance and bandwidth representations spelled out in the SLA?	☐	☐
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?	☐	☐

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?	☐	☐
4. Does using this product increase your in-office costs?	☐	☐
5. How often (and by how much) can the provider increase fees? _____		
a. Is there a cap on price increases?	☐	☐
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?	☐	☐
7. Have your compared the cost of the cloud service vs. non-cloud alternatives (present value calculation)?	☐	☐
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)?	☐	☐

As HP has stated in their publications, when moving to the cloud you have to think like a lawyer. Hopefully this checklist assists you in the considerations that should be undertaken prior to moving to a cloud-based service or application.

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

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