NOVA SCOTIA
BARRISTERS' SOCIETY

Cloud Computing Checklist Proposed Approach

Law Office Management
Standards Committee

Paul V. Saunders
November 24, 2021

LIANS/NSBS Solo and Small Firm
Virtual Conference 2021

Background

- The Law Office Management Standard Committee (LOMSC) is responsible for developing and maintaining the Law Office Management Standards for review and approval by the NSBS Council
- The NSBS receives many requests for guidance on the use of Cloud-Based Services given increased demand
- In 2019, the LOMSC was asked to undertake a review of the existing #6 - Cloud Computing standard to support Law Practices throughout the Province to help address this demand for support
- **Progress has been made, and the purpose of this Presentation is to seek feedback from you on the Proposed Approach**

Cloud Computing

- Cloud Computing (or on-demand computer services over the Internet) has become ubiquitous in law practice
- Practice management, email, and document storage applications are increasingly being deployed via the cloud in law firms
- Cloud-based services lower up-front costs and reduce the need for in-house expertise
- However, they raise significant issues of confidentiality, security and control of client data
- No longer an issue of whether they should be permitted but what is required of practitioners to navigate the risks

#6 – Cloud Computing Standard

New Proposed Wording:

A lawyer who uses Cloud Computing services for storing, processing, retrieving or transmitting client data must provide that reasonable care is taken to ensure that the data is at all times secure and accessible. The service provider and the technology used must support the lawyer's professional obligations, including compliance with the Nova Scotia Barristers' Society's regulatory processes1, and be in compliance with applicable privacy legislation, such as the federal Personal Information Protection Electronic Documents Act (PIPEDA).

This triggers the obligation to conduct due diligence on Cloud-based services

The Problem

- Large to mid-size firms often have dedicated IT resources that can help them navigate the challenges of transitioning to the cloud
- However, small firms and solo practitioners can struggle with this same process since they often don't have dedicated personnel to support them
- An analysis of potential services can be highly technical, and it can be difficult for practicing lawyers without expertise in this area to effectively manage the risks and engage in a meaningful dialogue with providers (they don't speak the same language)

Bridging the Gap

- The LOMSC struck a Tech Sub-Group composed of NSBS staff and tech-savvy lawyers with connections to IT departments and Managed IT Service Providers
- The group researched existing standards and resources
- Our focus was to help bridge the gap between smaller Law Practices/ Solo Practitioners and Cloud-Service Providers by focusing on the development of practical support tools

The Checklist

- While the group is in the process of updating the Standard (both above and below the line), it has also focused on the development of a Cloud Computing Checklist that could be used by Law Practices when assessing the use of a Cloud-Based tool
- Portions of the Checklist have been adapted from *The Law Society of Saskatchewan's Cloud Computing Guide*
- The Checklist has gone through several levels of review by the Tech Sub-Group, the LOMSC, IT security experts at larger law firms, NS-based Managed IT Service Providers, and several Cloud-based Service Providers
- **The Checklist is nearing completion, and the LOMSC is now looking for input and feedback from Small Firm and Solo Practitioners on the Checklist and the suggested approach**

Two Versions

- The Checklist has two versions:
  - **Cloud-Based Service Provider Version (For Completion by Providers)**
  - **Annotated Law Practice Version (For Use by Law Practices)**
- The intent is that Law Practices send a copy of the Provider Checklist to a Provider and ask them complete it by answering each as "Yes" or "No" with comments to explain any "No" answers
- Upon receiving the completed Checklist back from the Vendor, Law Practices can use the Annotated Law Practice Version to assist in reviewing their answers and assessing the risk

Provider Version

Step 1 - Providers answer "Yes" or "No" and provide comments as necessary and send back to Law Practice

#	Question	Yes	No	Comments
	INFRASTRUCTURE			
1.	Will Law Practice's cloud data and any backups and related infrastructure be located within Canada?	☒	☐	
2.	Does the Provider have a method to monitor for and report abuse of the cloud service (e.g. Denial-of-Service attacks)?	☒	☐	
3.	Does the Provider backup Law Practice data to a secure offsite location which is compliant with the same data security accreditations as the Provider's production data centre?	☐	☒	
4.	Is cloud data encrypted at all times including on any applicable mobile application, in motion over the Internet, and on the cloud (or at rest) with current encryption algorithms (including appropriate use of client-side vs. server-side encryption) and reviewed periodically?	☒	☐	
5.	Does the Provider utilize company-based security including intrusion detection and prevention and spam and virus filters?	☒	☐	
6.	Does the Provider use VPN or other encryption services for remote administration and are the encryption algorithms reviewed and updated periodically?	☒	☐	

NOVA SCOTIA
BARRISTERS' SOCIETY

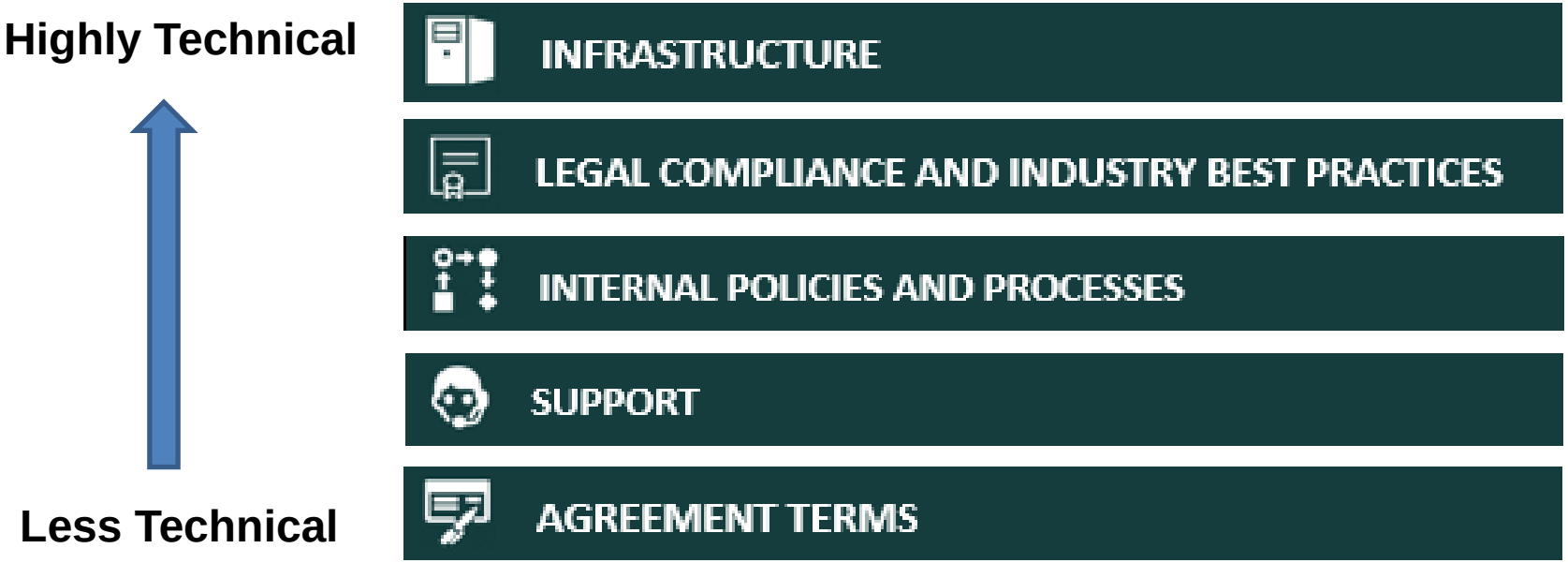
Annotated Law Practice Version

Step 2 - Law Practices assess Provider answers and seeks assistance if needed

#	Question	Yes	No	Comments
	INFRASTRUCTURE *The following questions are technical in nature. Some Law Practices will not be aware of the meaning of these questions, but most sophisticated Providers should be able to provide "Yes" to most, if not all, of the questions. Given the technical nature of these questions, it may be advisable to consult with a computer security expert or managed service provider the Provider does not answer "Yes" to the critical questions.*			
1.	Will Law Practice's cloud data and any backups and related infrastructure be located within Canada?	☐	☐	*Should generally be "Yes", but it would be permissible in the EU in most cases, but the US isn't recommended because of government based compliance policies (PIPEDA). May also be permissible if backups are encrypted.*
2.	Does the Provider have a method to monitor for and report abuse of the cloud service (e.g. Denial-of-Service attacks)?	☐	☐	*Always "Yes"*
3.	Does the Provider backup Law Practice data to a secure offsite location which is compliant with the same data security accreditations as the Provider's production data centre?	☐	☐	*Always "Yes"*
4.	Is cloud data encrypted at all times including on any applicable mobile application, in motion over the Internet, and on the cloud (or at rest) with current encryption algorithms (including appropriate use of client-side vs. server-side encryption) and reviewed periodically?	☐	☐	*Always "Yes". Generally speaking, client-side encryption prevents any third parties from viewing the unencrypted version of the data where server-side encryption enables the Provider to access the data.*
5.	Does the Provider utilize company-based security including intrusion detection and prevention and spam and virus filters?	☐	☐	*Always "Yes".*

Organization

- The Checklist has a total of 51 questions organized into five sections from most technical to least technical:



The more Technical the section, the more likely assistance may be required

Infrastructure – Samples

- *Will Law Practice's cloud data and any backups and related infrastructure be located within Canada?*
- *Does the Provider have a method to monitor for and report abuse of the cloud service (e.g. Denial-of-Service attacks)?*
- *Does the Provider utilize company-based security including intrusion detection and prevention and spam and virus filters?*
- *Does the Provider logically isolate Law Practice data from other tenants and management traffic?*

Compliance/ Best Practices – Samples

- *Is the Provider in compliance with all applicable privacy legislation and regulations in respect the collection, storage and protection of personal information?*
- *Is the Provider in compliance with a relevant security standard such as NIST CSF, ISO 27001, SOC or PCI DSS as demonstrated via certification with accreditation?*
- *Does the Provider implement change controls in accordance with reasonable industry practices including not utilizing production data in test environments?*
- *Is the Provider able to retain and/or archive cloud data for any Law Practice specified or legally required period?*

Internal Policies/Processes – Samples

- *Does the Provider have a policy and process to handle ransomware attacks?*
- *When Provider conducts a security investigation for a potential breach does it retain an investigation report for a period of at least two years thereafter?*
- *Does the Provider maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts?*
- *Does the Provider conduct security awareness and training for its employees at least annually (including phish testing)?*

Support – Samples

- *Does the Provider offer standard technical support during normal working hours?*
- *Does the Provider offer emergency technical support outside of normal working hours?*
- *In the event Law Practice discontinues its use of the service, will Provider provide Law Practice's cloud data in a format that can be moved to another cloud provider?*

Agreement Terms – Samples

- *Does the Provider's form of License Agreement (the "**Agreement**") provide that the Provider shall not share any of Law Practice's cloud data with other parties nor utilize any subcontractors or third-party cloud service providers without the prior written consent of the Law Practice?*
- *Does the Agreement ensure that ownership in any intellectual property rights to any cloud data are not transferred during the life of the contract and thereafter?*
- *Does the Agreement provide for any financial penalties payable to the Law Practice in the event the Provider fails to comply with the aforementioned representations?*

Practical Tips on Using Checklist

- The Checklist isn't exhaustive - other questions or issues may need to be addressed based on other factors such as the sensitivity or confidentiality of data
- If no confidential data is stored – the standard decreases (legal research, precedents, publicly available data, etc)
- Don't be afraid to reach out for assistance, ask colleagues and other law firms what they are using
- If the provider has all the recommended certifications, you should still ask all the questions, but that should give you a fair amount of comfort since they would need to have answered "Yes" to many of the questions to be certified
- Seek professional assistance is needed (focusing on more technical issues if required)
- Checklist is intended to be iterative, with periodic reviews and updates based on feedback (area is evolving so checklist should too)

Feedback

- If you would like to review the draft checklist email Paul Saunders (psaunders@stewartmckelvey.com) and ask for a copy
- Try the checklist out with a Provider and see how it goes
- Send any comments or feedback to Paul for review by the Tech Sub-Group and LOMSC
- **And… tell me what you think right now by asking questions or providing feedback using the chat feature**

NOVA SCOTIA
BARRISTERS' SOCIETY

Questions and Feedback

Do you think this resource would be helpful?

Does the proposed approach make sense?

Do you think you would use this?

How we can improve the approach?