IT.CAN ROUNDTABLE – OCTOBER 24, 2016
AUDIT AND BENCHMARKING CLAUSES
IN THE NEW POST-CLOUD, CYBER-SENSITIVE WORLD

FACT PATTERN

The Royal Toronto Montreal Canadian Dominion Imperial Bank of Nova Scotia and Commerce (the "Bank") has been looking to leading-edge technology startups to revitalize the way it does business. More particularly, the Bank is very interested in a US-based startup called mrtgg.ly, Inc. (the "Vendor") which offers mortgage processing services, including processing mortgage applications, credit review and approval and ongoing administration and servicing, including payment processing, along with a customizable on-line user interface which enables borrowers to update and retrieve information on-line, including amortization schedules. From the mtgg.ly website:

> Our value-added solution is disrupting the market and transforming the mortgage landscape. We leverage a hybrid solution utilizing customized, on-prem software components linked with a cloud-based service to provide the best of all possible worlds and give financial institutions the tactical edge they need to compete. Our proprietary, groundbreaking AI technology, coupled with our big data analytics and blockchain infrastructure, dynamically disintermediates mortgage intake and admin functions, drastically reducing time to market and increasing responsiveness, straight out of the box.

The Bank is very keen on the Vendor's solution and wishes to fast track the procurement. Business line representatives of the Bank have already had several meetings with the Vendor about its solution and how the Bank can implement it and have provided you, the Bank's legal counsel, with the following description (in case, in their words, you didn't "get it"):

> mrtgg.ly solution involves two primary pieces. First is their licensed software, which we will install and run on our servers. That software will require a fair bit of customization, primarily to accommodate differences in Canadian mortgages and to create links to our other systems. The second piece is their cloud-based service, which links up with the licensed software and provides analytics, credit review and an on-line portal for our borrowers. Fees will be charged on a subscription model based on the number of servers on which we install the licensed software, as well as the mortgage volume we process through their solution. The customization, along with some consulting and training, will be provided on a time and materials basis at their standard hourly rates. We plan to move all of our mortgage intake and processing to their solution in two months. As you know, mortgage lending constitutes a significant proportion of our overall lending activities.

Part 1

For some unknown reason, you feel compelled to consider only audit and benchmarking related issues. Within that scope, what issues or concerns would you raise given the above? What audit rights would you ask of the Vendor? What else would you ask of the Vendor?

Part 2

You have now received the Vendor's standard agreement, which the Bank has agreed to work with. You notice the following provision in their agreement:

> We reserve the right, from time to time, to conduct an on-site audit at any of your premises where you have installed or are using our software to verify your compliance with this Agreement. We may use a third party to perform such audit. You agree to cooperate and provide any assistance we require in connection with any such audit, including the provision of access to your hardware, systems and records that relate to our software or this Agreement, allowing us to run auditing software on your systems, providing us copies of all relevant records and causing your employees and agents to cooperate and assist, including responding to questions related to our software or this Agreement. If any such audit reveals any breach of this Agreement or any shortfall in the payment of any fees, you will immediately pay all expenses we incur in conducting the audit and any such shortfall at the then applicable list price, plus applicable interest and retroactive support and maintenance fees for a period of two years prior to the audit, in addition to any other remedies to which we may be entitled herein, at law or in equity.

What are your thoughts on this provision?

Part 3

Being the diligent lawyer you are, you have asked whether or not the Vendor undergoes a regular security audit. The Vendor replies: "Yes, of course we do. We undertake an annual SOC audit. Here's a copy." The audit report that they send you can be found in the attached Appendix.

You notice that the report identifies "Schmamazon Web Services, Inc." and not "mrtgg.ly, Inc." as the service provider. Puzzled, you ask the Vendor, to which they reply: "Yes, that's our cloud service provider. They're totally awesome. Everybody uses them. We use their computing, storage, database and networking services to run our proprietary cloud platform. When other users have asked, this is what we provide and they're usually fine with it."

What concerns, if any, would you have with what the Vendor has provided? How would you address each such concern?

Part 3 - Appendix

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design of Controls

To: Schmamazon Web Services, Inc. ("Schmamazon")

Scope

We have audited Schmamazon's description of its online storage system made available to user entities of the system for storage of user entities' data as of December 31, 2015, and the suitability of the design of controls to achieve the related control objectives stated in the description. Schmamazon uses several colocation service providers to host the computers used in its online storage system. The description includes only the controls and related control objectives of Schmamazon and excludes the control objectives and related controls of the colocation service providers. Our audit did not extend to controls of the colocation service providers. The description indicates that certain complementary user entity controls must be suitably designed and implemented at user entities for related controls at the service organization to be considered suitably designed to achieve the related control objectives. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities

On page 1 of the description, Schmamazon has provided a statement about the fairness of the presentation of the description and suitability of the design of the controls to achieve the related controls objectives stated in the description. Schmamazon is responsible for preparing the description and for its statement, including the completeness, accuracy, and method of presentation of the description and the statement, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design of the controls to achieve the related control objectives stated in the description, based on our audit. We conducted our audit in accordance with Canadian Standard on Assurance Engagements 3416, Reporting on Controls at a Service Organization, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our audit to obtain reasonable assurance, in all material respects, about whether the description is fairly presented and the controls were suitably designed to achieve the related control objectives stated in the description as of December 31, 2015.

An audit of a description of a service organization's system and the suitability of the design of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design of the controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to achieve the related control objectives stated in the description. An audit engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described at page 2.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in the storage of user entities' data. The projection to the future of any evaluation of the fairness of the presentation of the description, or any conclusions about the suitability of the design of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become ineffective or fail.

Basis for qualified opinion

As discussed on page 4 of the accompanying description, from time to time, Schmamazon makes changes in application programs to correct deficiencies or to enhance capabilities. The procedures followed in determining whether to make changes, in designing the changes, and in implementing them do not include review and approval by authorized individuals who are independent from those involved in making the changes. There also are no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes. As a result, the controls are not suitably designed to achieve the control objective, "Controls provide reasonable assurance that changes to existing applications are authorized, tested, approved, properly implemented, and documented."

Opinion

In our opinion, except for the matter described in the preceding paragraph, and based on the criteria described in Schmamazon's statement, in all material respects,

a. the description fairly presents the online storage system that was designed and implemented as of December 31, 2015, and

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively as of December 31, 2015.

Restricted use

This report is intended solely for the information and use of Schmamazon, user entities of Schmamazon's online storage system as of December 31, 2015, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when obtaining an understanding of user entities information and communication systems relevant to financial reporting. This report is not intended to be and should not be used by anyone other than these specified parties.

Audits 'R Us LLP

January 31, 2016
123 Gaap Lane
Saint-Louis-du-Ha! Ha!, QC

Part 4

It is now two years into the agreement with mrtgg.ly. The Bank is very happy with the solution. They are particularly happy because, shortly after they purchased the solution, they also purchased another cutting-edge solution from VMstuff, Inc. VMstuff's solution (which they call "SuprGiganticVM") allows its customers to create "super-sized" virtual machines that can span across hundreds, or even thousands, of physical computers. The Bank decided to install the Vendor's software on a single instance of SuprGiganticVM, which has, over time, allowed them to seamlessly scale their use of the software to just over 1,000 physical computers, under one single (but very massive) virtual server. This has also allowed them to save millions, as they have paid the Vendor the licensing fees for a single server.

The Vendor, puzzled about how the Bank has been able to handle such large volumes on a single server, has invoked its audit clause. Unfortunately, due to time pressures, you were unable to negotiate any changes in the provision, which appear in the signed agreement as you saw it earlier.

The Bank has come to you for advice on this request. How do you advise the Bank?