Appendix A: Cloud Service Assessment Guide

1. **General Considerations**.

   General considerations include what the Vendor is offering and a summary of some of the basic questions that should be asked.

   a. A detailed description of the DDSB information that the Vendor requires to perform their tasks and an acknowledgement that DDSB is the Information Owner.

   b. Does the CSP have an allowance to audit either the application or network infrastructure? What notice is required to do non-intrusive vs. intrusive scans or other vulnerability assessments?

   c. What allowances does the Vendor provide to access or request any security related configuration files, developed application code, or policy or quality assurance and testing documents?

   d. What internal software/hardware/infrastructure audits does the Vendor perform and what actions do they take upon locating a security issue?

   e. Explain how the Vendor designates a customer contact in the event of a breach or security issue?

   f. Does the Vendor use DDSB Confidential Information for any other purposes, whether metadata (in part) or whole for other services?

   g. Description of scheduled maintenance times and customer notification processes. Any maintenance history provided is helpful.

   h. Explain the Vendor's levels of customer support for your Cloud Services offering beyond knowledge base, FAQs, or message boards. Are there additional costs associated for this support? If so, note those costs.

   i. Define the Vendor's trouble ticket severity levels. How are they assigned and how are they escalated? Is escalation automatic based on a metric or customer initiated?

   j. Service Level Agreement for uptime. Targets should be 99.99% if possible but may vary. For DDSB guidance:

      i. 99.999% uptime translates to 5.39 minutes per year of downtime

      ii. 99.99% uptime translates to less than 53 minutes per year downtime

      iii. 99.9% uptime translates to almost 9 hours per year downtime

      iv. 99.5% uptime translates to almost 44 hours per year downtime

      v. 99% uptime translates to almost 90 hours (87.6 or 3.65 days) per year downtime

   k. Mobile device access capabilities and any security controls for protecting linking to lost or stolen customer mobile devices containing data.

l. Review the Vendor Personnel hire, orientation, and security training process and any non-compete or data/customer confidentiality agreements you have them sign.

2. Data Encryption

Both data in transit and data at rest require encryption to adhere to most governmental regulations. Types of encryption and protocols should be assessed.

a. Data in transit and file uploads or transfers must be secured with encryption protocols. Those protocols utilized should be explained by the Vendor.

b. For data in transit, CSPs should be using Transport Layer Security (TLS 1.2) from an established, reliable and secure independent certificate authority (CA). The TLS 1.2 CA needs its authentication practices audited annually by a trusted third-party auditor. The CA needs its authentication practices audited annually by a trusted third-party auditor.

c. For data in transit, TLS should deliver at minimum 256-bit encryption based on the new 2048-bit global root. And it should require a rigorous authentication process. The certificate issuing authority should maintain military-grade data centers and disaster recovery sites optimized for data protection and availability.

d. For data at rest, what encryption technology is utilized for data storage?

e. For data at rest, how are encryption keys for stored data managed?

f. Particularly for data backup and recovery, what technology is used to encrypt data backups and how are those keys managed?

g. If databases are utilized, to what level is encryption applied?

3. Access Privileges

CSPs should be able to demonstrate they enforce adequate hiring, training, oversight and access controls to enforce administrative delegation.

a. A description of the physical security measures in place within the Vendors data centers. Describe both the physical data center access as well as server room and physical host access.

b. How are the logical and physical data center services secured from other users and from external threats?

c. What level of support does the Vendor provide for Single-Sign-On (SSO) or authentication utilizing DDSB identity management infrastructure?

d. A detailed description of those authentication methods.

e. Any support for two-factor authentication?

f. What level of administrative privileges and controls does DDSB IT Services have over the system or software and its users?

4. Regulatory Compliance

Information Owners are accountable for their own data even when it is in a Public Cloud Storage Service and should ensure their CSPs are ready and willing to undergo audits and provide proof of such audits.

a. What is the Vendor's and any 3rd party's compliance requirements to SSAE 16/SAS70-II, SOX, PCI-DSS, ISAE3402, SOC1, 2 or 3, Safe Harbor, or other regulatory certification requirements?

b. Can the Vendor describe the commitment to their and any 3rd party utilized to remain in such compliance?

c. Will the Vendor attach their latest compliance audit performed by a recognized qualified 3rd party and commit to maintaining that described level of security?

d. What ISO standards do the Vendors adhere too?

5. Data Provenance

When selecting a CSP, ask where their datacenters are located and if they can commit to specific privacy requirements.

a. A description of how often is infrastructure/hardware/software upgraded, hardened and patched and what communications/requirements are there with the customer?

b. Describe the automated Information Lifecycle (Configuration Upgrade and Control) Management capabilities of Cloud Service offering and the benefits clients receive from this functionality.

c. What are any options for dedicated storage, dedicated hardware firewalls and load balancers to connect to the Public Cloud Storage Service offerings in the Vendor's facilities?

d. Can you share networks, VPNs, firewalls and load balancers between the Vendors dedicated and Public Cloud Storage Service environments?

e. Explain your data and sensitive documents handling and destruction practices for customer data.

f. Define where geographically data is stored and ensure that it complies with MFIPPA, PHIPA and the Education Act.

6. Data Segregation

Most Public Cloud Storage Services are shared environments, and it is critical to make sure hosting providers can guarantee complete data segregation for secure multi-tenancy.

a. Provide an overview of the dedicated single-tenant and shared (multi-tenant) Cloud Services provided by the CSP.

b. Notation if the data center components are provided by Vendor or by another third party

and a description of maintenance or transfer of those services.

c. As a customer, how are we responsible for entering or transferring data?

d. Explain how data is either physically or logically separated such that one account cannot see data from any other account.

7. Data Recovery

Ensuring that the hosting provider can do a complete restoration in the event of a disaster.

a. Describe the SAN and/or NAS storage options connected to the Cloud Service.

b. Describe the backup and archival process and length of time backups are available.

c. Does the CSP perform test restores?

d. Does the CSP have any file or directory versioning capability or capabilities short of restoring from a backup?

e. Location of backups and key management and storage for any backup encryption keys.

f. What archival backup/restore/versioning is part of the agreement and what actions require any additional service fees?

g. Explain any shadowing or redundancy the Vendor has across multiple datacenters or repositories, the geographic location of those data repositories and whether the data repositories controlled by the Vendor.

h. An explanation of the Vendor disaster recovery plan with maximum downtime limits.

i. Does the Cloud Service offer persistent Cloud images (longer than 2-week retention) or offer back up in the Cloud Service longer than 1-month retention?

j. Does the Cloud Service backup allow file based restore, without requiring clients to mount a full historic copy of their virtual machine?

8. Monitoring and Reporting

Monitoring and logging Public Cloud Storage Service activity is difficult to do. DDSB employees should ask for proof that their hosting providers can support investigations.

a. Explain how the Vendor monitors and reports upon notification of abuse or investigation. This might include notices to the Information and Privacy Commissioner of Ontario, criminal or civil investigations and additional requests made by either an outside entity or the DDSB.

b. Explain the dashboards and analytics that are in place for customer use.

c. Explain any real-time monitoring that the customer might deploy that the Vendor has developed.

d. Explain what additional reporting, training, aggregate, industry, research, or other reporting

information or data might be available as part of a customer subscription.

e. Define and secure documentation on Vendor's policy in case of a data breach.

9. Business Continuity

Businesses come and go, and DDSB employees should ask hard questions about the portability of their data to avoid lock-in or potential loss if the business fails.

a. Does the Vendor have a formal Risk Analysis plan that is reviewed annually?

b. Does the Vendor have a disaster recovery plan?

c. What tests does the Vendor perform to audit their disaster recovery plan?

d. What are the contract stipulations for potential customer losses or for transfer of data and support to another organization should the business fail?