BRUNO COLIN & JOHN VAN LOENEN

A practical guide to cloud computing services

Cloud computing is a rapidly growing area which offers economies of scales and new choices, but companies need to guard against the risks.

The popularity of cloud computing services has grown immensely as research firms look to quickly deploy and use computing infrastructure without owning any physical assets. Firms no longer need to invest in data centres, hardware, software and the staff to support them, and can concentrate on their core offerings.

With opportunity, however, comes risk. Here are some key steps to help researchers and research companies mitigate potential liabilities and optimise the decision-making process.

This guide is intended for any person or enterprise entertaining the idea of using the cloud. We recommend that it be made available to all staff members. The guide will be updated and expanded on a regular basis.

Cloud computing services (CCS) generally follow one of two models:

Public cloud A computing infrastructure that is not restricted to any one geographical environment or region. With shared resources, it can be quickly scaled up or down and is extremely efficient, as enterprises pay for what they use. Data may reside in one or several regions at the same time. Major concerns include security, reliability and regulatory compliance.

Private Cloud A computing infrastructure defined by a set geographical environment or region, with resources strictly dedicated to an enterprise. Security and reliability are contractually agreed upon and a high degree of regulatory compliance is built in. Private cloud is more expensive and cannot be scaled up or down as fast as a public cloud.

WHAT YOU NEED TO KNOW

Regardless of which model you choose, you need to understand what data you will be storing with your CCS provider and take a common sense approach to risk. Furthermore, it is vital to ensure that all privacy and data protection statements are clear, known and under control.

1. Read and understand the Master Service Agreement (MSA) with your CCS provider before signing. Ensure that a non-disclosure agreement is in place.
2. Ask your CCS provider to perform regular due diligence if it uses third-party vendors.
3. Ensure that a Data Processor Agreement is in place with the CCS provider.
4. Understand what privacy and data protection requirements you are obligated to adhere to in your local jurisdiction, and confirm the commitment of the CCS provider to these requirements in the MSA.
5. Be aware that, if stored in a CCS, your data may be co-mingled in storage, on disk and tape, with that of other companies. Check your obligations under existing client contracts to determine if your data needs to be segregated.
6. Understand what will happen to your data once your engagement with the CCS provider has ended. As some will retain data indefinitely, it is essential that your data is completely removed and expunged from all systems, disks and tapes when no longer being used for your service. Ensure that a clause to this effect is included in the MSA.
7. Ensure that the CCS provider conducts annual information security audits for best practices and procedures.

8. Ask for a vulnerability test/scan when the CCS is provided through a web platform. If the provider cannot conduct a scan, perform your own.
9. Ensure that the CCS computing infrastructure has an annual audit of security controls, processes and procedures. Well known auditing standards are SAS 70 Type II, ISO 27001 and Systrust.
10. Ask for details of the CCS provider's Business Continuity Plan and their backup procedures to ensure they have an adequate level of business continuity and regular backups and restores. Ensure that backup tapes are securely rotated offsite and are subject to a strict and documented chain of custody.
11. If your CCS provider replicates its data offsite as part of its backup strategy, understand where it is being replicated to. Ask to have another copy of your most important data stored locally or with a different service provider.
12. Understand what type of customer/technical service is provided and how it is delivered, eg 24x7 telephone versus 9 to 5 e-mail support.
13. Make sure your CCS provider details its Service Level Agreements (SLA) for the various facets of their offering (network uptime, hardware failure, etc.) in the MSA.
14. Understand what the service credit policy is if an SLA is not reached; a good CCS provider will credit a customer when an SLA is not met. **RW**

GLOSSARY

Cloud computing: The use of computer resources (data, software) via a web-based computer network. Clients can submit a task to the service provider without owning the software or the hardware. Software as a Service (SaaS) describes programs offered through the cloud by a software provider.

Chain of custody: Chronological documentation showing the custody, control, transfer, analysis, and disposition of any physical or electronic asset.

Data processor (or processing) agreement (DPA): Data processing is the act of converting data into information. A DPA defines certain service levels to be applied to all data services and processing provided by the supplier. In many cases in the market research industry, this agreement provides for an adequate level of data protection when personal data is transferred from the EU to third countries.

Master Services Agreement (MSA): A legally binding contract between two or more parties which goes into immense detail regarding the basis of the usually service-oriented contract.

Non Disclosure Agreement (NDA): A contract to protect information considered to be confidential whereby the parties involved promise not to divulge this information.

Service Level Agreement (SLA): A contract between a provider and a customer that specifies in measurable terms the services to be provided. This usually includes contracted delivery time and quality performance indicators.

Vulnerability scan: An automated tool that checks computer systems for vulnerabilities. The tool remotely reviews networks and web applications based on Internet Protocol (IP) or Uniform Resource Locator (URL) addresses.

Bruno Colin is global managing director of Operations & IT and member of the Global Custom Research Board at GfK Custom Research. **John van Loenen** is global information security director at IPSOS. They are both members of ESOMAR's Legal Committee.