AskAvanade: Answering the Burning Questions around Cloud Computing

There is a great deal of interest in better leveraging the benefits of cloud computing. While there is a lot of excitement about the cloud, there are understandably some common questions and this document addresses them.
Avanade is one of the leading global providers of Microsoft based technology consulting and in particular Cloud Computing Services based on the Microsoft platform. Using our extensive customer implementation experience we have collated answers to the burning questions we hear from our customers daily, from EU Data Privacy to security regulations, all which will better assist you as you as you plan for and implement the right cloud solution for your organization.

1. What is “cloud computing?”

Cloud computing is a model providing convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction, and consumed on a pay-per-use basis. When planning for cloud solutions you will want to consider the common features that can benefit your organization including:

- On-demand self-service: You can provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service’s provider.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, smartphones).
- Resource pooling: Computing resources are typically pooled to serve multiple consumers, using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence, in that the user generally has no control or knowledge over the exact server location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., region, country, data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- Rapid elasticity: Capabilities can be rapidly and elastically provisioned – in some cases automatically – to quickly scale out and rapidly released to quickly scale in. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both provider and consumer. There are several layers of cloud service, consisting of infrastructure, platform and software. These are offered cumulatively; i.e., platform services include infrastructure services, and software as a service includes embedded infrastructure and platform services.

<table>
<thead>
<tr>
<th>Cloud Offering</th>
<th>Hosting</th>
<th>Infrastructure</th>
<th>Applications</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>IaaS</td>
<td></td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PaaS</td>
<td>P</td>
<td></td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>SaaS</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>

©2012 Avanade Inc. All rights reserved.
Cloud services can also be categorized based on how the cloud infrastructure is made available. Avanade offer different types of cloud service offerings, depending on the different needs of our customers:

- **Private cloud:** The cloud infrastructure is operated solely for our customer. Infrastructure may be managed by our customer or by a third party and may exist on premises or off premises. (The "private" descriptor emphasizes dedication to specific customer, rather than any statement of greater level of security etc.)
- **Public cloud:** The cloud infrastructure is available to the general public or a large industry group and is owned by an organization selling cloud services as a common utility service. However each customer still comprises a fully logically and virtually separate "tenant" within the common infrastructure.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

2. **Who is responsible for data security in the cloud?**

We take a different approach to our respective security responsibilities depending on whether we are providing IaaS, PaaS or SaaS cloud services. Because many standard security controls are applied at the application layer or in the data store, both of which are typically owned by whoever controls the software application, often our customers retain control of and responsibility for many specific security functions. In the IaaS and PaaS models, many standard security controls, such as backups, encryption, access management, logging attributes and IDS, must be provisioned and executed by the customer. When Avanade controls or provisions the application, we will likely need to execute these security controls on your behalf.

Responsibility for cloud security is generally allocated among Avanade, our preferred cloud service providers, and you, our customer. The manner in which this responsibility is delegated will depend on the specific solution.

Specific categories of requirements correlate to which party controls which portion of the computing infrastructure. For instance, the preferred cloud service providers will be responsible for physical security in all cases, and for securing access to hardware in all cases other than co-location deployments. Whoever controls the application will, necessarily, be the party who must deploy application-level security measures. This could be a SaaS cloud service provider, Avanade as a system integrator, or your IT team, depending on the extent you manage the application. The specific service model selected and the specific regulatory regimes applicable to your data will determine the allocation of security responsibilities.

Whether the cloud service provider has logical access to data and under what circumstances is a significant driver for the specific requirements that need to be flowed down to the cloud service provider. For instance, in some cloud scenarios, the cloud service provider has super-user access rights that enable it to override all other users to get logical access to the data on its systems. In other scenarios, the customer may have “dominant” super-user rights and may provision cloud service provider personnel with access in the same way it would provision its own administrators’ access. In these scenarios, the cloud service provider doesn’t have any logical access to data that the customer doesn’t expressly grant to it. Under this model, the customer also has the ability to establish the logging attributes and audit procedures and to monitor the service provider personnel activity on the system, and can shut down the cloud service provider’s access at any time.

3. **What happens to my data in the cloud?**

This will depend on the cloud service model you choose. Generally, the financial and functional efficiencies of cloud computing increase as you use a more standardized model (e.g., public cloud). To the extent you choose to physically segregate your data and to control where the data resides at any particular time (e.g., private or hybrid cloud), you will likely realize fewer efficiencies.

At a very basic level, the customer sends data over the Internet to our cloud service data server, which then stores the information, generally in a dynamic, virtualized storage medium (instead of dedicated hardware). When you want to use that information, you access the cloud service data server through an online interface. The server then either sends the requested data back to you or allows you to access and manipulate the files on the server itself.

In a private cloud setting, you own or lease the specific hardware and software used to provide the services. In a public cloud setting, the cloud provider will control the hardware and often the operating system, and sometimes also the software, depending on whether IaaS, PaaS or SaaS cloud services are being provided.

4. **Can I ensure that data will only be hosted in the European Union? Where is the hardware stored?**

While it may be possible to limit use of servers in countries outside of the European Economic Area, doing so will eliminate some of the efficiencies associated with cloud-based services and likely will increase the cost to you. In most cases, even when data is stored in Europe, administrative or support personnel located outside the EU have the ability to access data stored on the servers. If restricting data to servers located in the European Economic Area is imperative to your cloud-based services, we will work to accomplish this end. However, as noted, it may affect the efficiencies and the cost of the services to be delivered.

If you are EU-based and personal data is accessible outside of the EU, then we will agree to execute EU Model Clauses with your company. In addition, we have preferred cloud service providers with whom we have already signed EU Model Clauses. You may wish to consider other options, such as data encryption or anonymization, to provide greater security when data originates from Europe.

5. **If data is not stored within the EU, how can I be sure that my data is handled with the same level of data protection as in the EU? How can we ensure that we meet EU data privacy requirements?**

If you are concerned about meeting EU data privacy requirements we will enter into appropriate data processing agreements with you, as well as ensure that we are providing cloud services to you using preferred cloud service providers who have entered into EU Model Clauses with us. Currently a limited number of our preferred cloud service providers have agreed to accept EU Model Clauses, including Microsoft®(Azure™ core services / Office 365), Terremark®, Verizon Business and NTTA.

©2012 Avanade Inc. All rights reserved.
6. Can I use a cloud service for Protected Health Information (PHI) covered by HIPAA or government information?

Yes. We can ensure that cloud services use preferred cloud service providers who have entered into business associate agreements with us. Currently a limited number of our preferred cloud service providers have agreed to accept the business associate agreement terms, including Terremark®, Verizon Business and NTTA.

You will need to understand the specific government regulations that are imposed by the jurisdiction in question, which may vary considerably. In general, U.S. federal government rules permit using cloud services to host lower-sensitivity data. Accenture Federal Services offers an NTT Data solution that permits greater flexibility.

You will need to evaluate cloud service offerings for other regulated data on a case-by-case base to determine whether these service offerings are appropriate for you.

7. Should we be concerned about export restrictions if we are a U.S. company?

In general, U.S. export enforcement agencies have provided little guidance with respect to cloud computing. The determination as to whether a cloud computing system hosting EAR- or ITAR-controlled technology or technical data remains case-specific, and there is general agreement that users and providers of cloud computing solutions should proceed cautiously. The U.S. Bureau of Industry and Security (BIS) has issued several advisory opinions, which generally seem to place the onus for export compliance with the user. As with the other restrictions above, this obviously only applies to the subset of your data which matches those attributes.

8. Does the provider have a right or the ability to access or use the data?

Unless contractually agreed upon, our preferred cloud service providers are only permitted to access cloud consumer data as necessary to provide the service and improve their ability to deliver the cloud services.

Whether or not a cloud service provider has logical access to the data will impact whether the service provider has the ability to access data. Not all cloud providers have this ability by default. Please also refer to the discussion about different “dominant” administrator models in question No. 2 above.

9. Can other customers see/access our data?

No. Virtualization is very reliable and only parties who have been granted access rights will have the ability to see or access your data. The virtualization layer ensures that no customer has the ability to “see outside their own boundaries”.

10. Who actually does have access to the data or the hardware the data is stored on?

This will be determined by the nature of the cloud service offering you select. A cloud service provider will almost certainly have access to the hardware on which data is stored, but one effect of virtualized storage is that access to hardware generally does not by itself provide logical access to stored data. Our contracts with our preferred cloud service providers limit access to authorized personnel and provide for specific procedures to be followed (and strict limitations governing) when preferred cloud service provider personnel or contractors access your data. No matter where your data is stored or accessible, it is always possible that a regulator or court of competent jurisdiction might attempt to access data (a) maintained on a service provided by a cloud service provider that is within its jurisdiction, (b) accessible by a cloud service provider or third party within its jurisdiction or (c) maintained on computing equipment within its jurisdiction. In appropriate circumstances, where particularly sensitive data is involved, you may wish to consider encrypting cloud-based data using strong encryption with keys that you, rather than the cloud service provider, maintain. Please also refer to question No. 2.

11. How will the transfer of data from the company into the cloud be secured? Is it safe?

Our contracts with you and our contracts with our preferred cloud service providers carefully address data and service migration issues. In many IaaS and PaaS settings, our customer is responsible for all application or data-level security, including encryption at rest and during transmission. Some cloud standard service offerings may not include encryption or VPN tunnels between data centers where storage is done on a multi-data center or regional basis. When these are not part of the standard service offering, Avanade can offer the ability to add these additional security measures.

12. How do you ensure security/privacy of our data in the cloud?

For all the concern about data security in the cloud, our preferred cloud service providers may be better situated than an individual company to implement robust security measures and maintain security expertise in-house. Certainly every cloud provider goes to market knowing that its infrastructure will be targeted by hackers, malicious code, and the full suite of cyber-risks. Thus security is a business-critical issue for our preferred cloud service providers, which creates strong incentives to pursue and maintain robust, cutting-edge security. In addition, it is generally easier to manage and respond rapidly to software and application vulnerabilities in a cloud environment.

The more difficult issue at times can be obtaining the necessary contractual provisions from cloud service providers that enable the customer to demonstrate its compliance with its legal requirements under data privacy laws. Many companies with regulated data have faced challenges negotiating satisfactory terms with cloud service providers. Avanade and Accenture have been able to address a number of data privacy regulatory concerns with many of our preferred cloud service providers to reach more favorable terms, from a privacy and security perspective, than are frequently available in the marketplace.

13. Who will be liable if data is missing or accessible to unauthorized people? (Leak of data)

While we have been successful in negotiating higher than standard limits on liability with several of our preferred cloud service providers, liability is still in most cases capped at relatively low levels. The limited recovery from
cloud providers may affect the overall risk profile of IT services, but this must be balanced against the economic benefits of cloud computing, which can be significant. Also, the change in risk profile may be more perceived than real, because the actual security deployed by cloud providers is robust.

14. If data will be stored in the U.S., how can I be sure that public authorities will not access my data?

There has been a lot of press about the threat of U.S. government access to cloud-stored data through the Foreign Intelligence Surveillance Act of 1978 (FISA) “business records” orders and U.S. National Security Letters under the Patriot Act. These mechanisms may be more streamlined than traditional warrants and subpoenas, but they do not significantly expand the kind of data that can be accessed by law enforcement. There are significant legal and procedural limitations on the data that can be accessed using these mechanisms. Further, these U.S. legal processes are not fundamentally different from what we see in other countries. While some of this information is not publicly available, evidence to date suggests that U.S. law enforcement is more likely to rely on established international cooperation channels to obtain data than it is to pursue data in the custody of service providers. In appropriate circumstances, where particularly sensitive data is involved, you may wish to consider encrypting cloud-based data using strong encryption with keys that you, rather than the service provider, maintain.

15. Will public authorities be allowed to access data in European countries?

Law enforcement in the EU is likely to have jurisdiction over data stored in the EU or on cloud services provided by entities that are subject to their jurisdiction. Even where data is not physically present in, or accessible from a particular country, a regulator may attempt to obtain data by asserting jurisdiction or using mutual legal assistance treaties or other international discovery tools. In appropriate circumstances, where particularly sensitive data is involved, you may wish to consider encrypting cloud-based data using strong encryption with keys that you, rather than the service provider, maintain.

16. How long do you keep the data? If the agreement is terminated, do you delete all data?

Our customers typically control the disposition of data. This means that when you no longer use the cloud environment, the data is no longer retained. The recoverability of data on the hardware used in the cloud environment is mitigated by the virtual nature of the cloud environment (e.g., wiping, rewriting), which we contractually require of all of our preferred cloud service providers.

17. Can we audit the process to ensure our data is being processed according to the contract?

This depends on the circumstances. For security and contractual reasons, we are unable to permit our customers to audit public clouds or public cloud facilities. To the extent permissible, we will share independent security audits of our preferred cloud service providers with our customers. Independent audit certifications such as ISO27001 series will show that the cloud provider is taking the necessary steps to identify and mitigate risks. Inside the service being provided, (e.g. PAAS/SAAS), we require our preferred cloud providers to provide extensive audit hooks for reporting, (e.g. last logged on etc)

18. How are security protocols being managed?

Avanade, an affiliate of Accenture Inc., employs the cloud services security strategy developed by Accenture Cloud Enterprise Services (CES) for cloud providers leveraged through CES or through other preferred cloud service providers. This is being implemented in cloud service provider contracts pursued by Avanade and Accenture.

In particular, our Security Protocols Schedule contains a detailed set of specific contracting requirements that address data governance, organizational security, physical security, and technical security requirements. This schedule is designed to ensure that security responsibilities are clearly identified and allocated between the data owner and the cloud service provider. Avanade and Accenture work with preferred cloud service providers to offer you various types of cloud solutions. Many of our preferred cloud service providers have accepted our Security Protocol Schedule in whole or in part.

You will need to evaluate your use of Avanade’s cloud service offerings on a case-by-case basis to determine whether our service offerings are appropriate for you.

If you have additional questions around Cloud Computing or require further information on our Cloud Computing experience in your industry and country, please contact gavin.williams@avanade.com.