Ten Things to Ask Your Vendor
Before Entering the Government Cloud
Introduction

Over the past decade, the semantics surrounding what we now call cloud computing have evolved. In the late 1990s, the term application service provider (ASP) was common, and then on demand was the accepted parlance. This was followed by software as a service (SaaS) and then, most recently, the cloud.

Cloud computing is a broader, more encompassing term. ASP, on demand, and SaaS reflect variations in how an application is built and then licensed to others as needed, like a utility. Cloud computing also encompasses concepts like elasticity, massive scalability, and multitenancy as well as infrastructure and platform-as-a-service (PaaS) capabilities. Advancements in technology and internet bandwidth have created more variables and possibilities than ever before for government agencies.

The advancements that have taken us from ASP to cloud concepts like SaaS are increasingly seen as revolutionary. With cloud computing, we are able to deliver a higher-quality service with better economics. Economies of scale and automation drive faster ROI and better experiences. Advancements also have brought some change in how IT management engages with a cloud computing provider.

This white paper contains 10 questions based on best practices that we have gathered from our analysis of the industry, including government agencies, and our direct experience with numerous cloud deployments in the public and commercial sectors. These questions come from conversations with CIOs, program and project managers, directors of IT, engineers, developers, administrators, and every other IT role you can imagine, in every industry and with every size of company.
Evaluating and Selecting a Cloud Computing Provider

As we closed out the first decade of the twenty-first century, hype around SaaS and cloud computing was at a fever pitch. Hype, while great for exposure and recognition, can also be a detriment to successful adoption of a solution or technology. Hype often comes paired with inflated expectations, misunderstandings, and even disillusionment. This white paper is a guide on how to engage with a cloud computing provider in a way that separates the propaganda from the reality of their solution, focusing on things that are important to IT organizations as they look toward a successful deployment of cloud-based services.

Interestingly, even with the “utility” promise of cloud computing, the approach that IT uses to evaluate and select a service or solution hasn’t really changed. CIOs and IT organizations still need to focus on finding the right solution for the operational needs. As before, you should start with a comprehensive understanding of the operational requirements. Then move on to a good understanding of the appropriate enterprise architecture, including a determination of selecting a commercial solution versus building in-house, and deciding whether or not a best-of-breed versus a monolithic solution strategy is right for your organization. If your selection criteria lead you to a solution that is provided in the cloud, these 10 questions will provide a head start in the analysis.

Here are some of the underlying questions you should ask a cloud vendor:

- Do you offer the best cloud solution, both functionally and economically?
- How secure is your cloud? Does it meet government security controls and standards?
- How easy will it be to do business with you? What are your long-term prospects as an organization?
- Does this cloud solution really reduce my technology complexity?
- Am I able to effectively manage my operational, security, and compliance risks?

How do you know if the promise will live up to the hype? Ask any cloud vendor you are considering the following 10 questions in addition to your structured evaluation.

1. Can You Demonstrate Real-World Successful Deployments Similar to Mine?

Most vendor solutions look good on paper, but the proof is always in the pudding. When you’re trying to manage deployment risk, there’s nothing more comforting than knowing you’re not the first one to implement the specific configuration you are planning. Look for relevant examples of functional and ROI/business value proof points. Look for third-party confirmation through awards and the stories that go with them. The vendor should be able to tell you how other organizations have used their solution to solve the same operational challenges you’re trying to solve.

Ask the cloud vendor for customer references. Find your own references through your network. If you’re like most government leaders today, you’re being asked to do more with less, so understand how the cloud vendor’s current customers have been able to do the same.
2. Do You Have a “Try-Before-You-Buy” Program?

One of the unique things about cloud computing is that you have an opportunity to enlist the vendor to help you convince management that the ROI/business value potential is there. The ability to test the concept first helps allay fears and hesitation before you sign a contract. Specifically, ask about the ability to pilot the solution. You may still need to pay for implementation services associated with the pilot, but in this brave new world of cloud computing, look for proof points and results up front before you make the large investment.

3. Do You Offer Contractual Flexibility and Price Protection?

Many of the bad licensing practices that occurred in the on-premises enterprise software world have now found their way into the cloud. For example, “shelfware” remains a significant problem because organizations are forced to buy more than they need to up front, even though a cloud computing environment should provide for rapid elasticity. Although the massive scale of a cloud computing provider should help to smooth out financial unpredictability, organizations are also forced to commit to interminable contracts to get any sort of pricing predictability. Cloud computing subscriptions are supposed to eliminate the vendor lock-in associated with perpetual licensing, but time and time again we see long-term contracts being deployed for cloud services. There are at least three key questions to ask about contractual flexibility and price protection:

- Do you provide a standard annual termination for convenience?
- Do you allow for annual usage-level alignment (up or down) based on my business needs? Can I apply monthly “rollover” usage to address seasonal peaks?
- Do you provide long-term price protection?

Cloud computing offers a lot of promise and disruptive innovation in how software is consumed and acquired. Much of the hype of cloud computing is around the increased alignment between the cloud service provider and the client, driven because of the subscription model and speed of innovation. Make sure your cloud vendor isn’t diluting that promise by living in the perpetual-license past.

4. Do You Have Service-Level Agreements and a Strong History of Service-Level Performance?

Service-level agreements (SLAs) are another great way to create alignment between a service provider and a client. Although you don’t want to depend exclusively on the SLA for alignment or performance, they are a necessary backstop, and putting effort and thought into getting them right is important. A mature and professional cloud computing provider should be giving you what you need out of the box. There are five things you need to keep in mind:

1. Are the SLAs relevant to the areas that need alignment, such as availability, transaction time, storage, and performance?
2. Are the SLAs relevant to what they’re supposed to be accomplishing? Cloud is typically a subscription model of service licensing. You’re not buying a perpetual license but the right to use...
the software for a period of time. The business model of most cloud computing providers has built-in incentives that align with your satisfaction and success. Most of these operational models depend on your renewal. This is one of the advantages of working with a cloud provider, because they put their subscription revenue at risk, not just their maintenance and support revenue. Because of the broad alignment that the subscription model creates, the SLA can be focused on a few key high-risk areas.

3. Make sure there is broad visibility into the situations where there might be some breach of the SLA. In other words, how transparent is the vendor in sharing their actual SLA performance on a daily, weekly, or monthly basis?

4. Are the SLAs results oriented? The SLAs should help you.

5. Most importantly, if the vendor drops the ball and misses SLA performance objectives, are they willing to “put their money where their mouth is” and compensate you financially? You need more than lip service.

The point of the SLA is not to replace trust. The subscription model creates a strong enough general incentive for performance. The SLA needs to be there to define the minimum acceptable levels of performance and ensure that, in the case of a failure, appropriate action is taken. Think of the entire value chain in your business, and make a small list of critical metrics to reflect in your SLA. No provider is perfect—what you want is for them to be serious about a systemic fix to any issue that arises, and SLAs can be very useful in achieving that. And you want them to be accountable for not meeting objectives.

5. Do You Provide Operational Transparency?

It may seem strange, but cloud companies sometimes forget about the service part of the equation. You get the functionality, you get professional services, you get some access to support, but if mission-critical software is involved, you need more. If the services you’re getting are a black box and there’s an issue, it’s very difficult to understand the source of the problem—particularly in an integrated system. Many cloud providers will give you visibility that their overall service is up or down, but that is significantly less “service” than you’d have if you were running the solution on premises. Look for visibility into these services at a minimum:

- Monitoring and operational management
- Performance management
- Change management
- Capacity and license planning and usage management
- Problem management
- Service-level management
- Service-level data integration
Keep in mind that you will likely not get approval rights into a cloud computing provider’s change management or capacity management processes, but they should be willing to provide visibility into these services. They are, after all, performing them on your behalf, and a part of your organization is running on their platform. Transparency is exactly what helps to build trust, and it also provides a powerful incentive for the provider to maintain excellence in their operations. Make sure your cloud vendor is committed to both excellence and transparency.

As a government agency, you also have the right to request and review the provider’s Certification and Accreditation (C&A) packages. At a minimum, the vendor should comply with the National Institute of Standards and Technology (NIST) 800-53 Moderate Controls.

6. How Do You Instantiate Multitenancy in Your Cloud Offering?

Multitenancy is simply the ability to run multiple organizations across a shared infrastructure environment. There are different approaches to achieving multitenancy. In the world of technology, as soon as we align with one particular technology, something new and better comes along to replace it. The point of multitenancy is to ensure optimal use of hardware with the goal of improving usage efficiencies at lowered overall costs. Multitenancy allows the provider to run a highly homogeneous infrastructure, creating a number of operational and cost advantages. Find out if the multitenancy approach the provider uses achieves this goal. Many ASP vendors have gone out of business because they were not able to deliver the type of efficiencies and reduced systemic risk that today’s cloud vendors can.

Multitenancy makes the economics behind the cloud work. The more efficient the multitenant model is, the better your pricing should be. Of course, it is not all about cost, and you need to weigh this against the risk posture of this environment. There are better and worse approaches to multitenancy when it comes to efficiency. There are also better and worse approaches when it comes to risk management. This is worth exploring as part of your evaluation.

7. Do You Have a Comprehensive Disaster Recovery Plan?

There are actually three questions in this area that you should ask a cloud vendor:

1. Do you have a disaster recovery (DR) plan?
2. Do you test your DR plan?
3. Does your DR plan actually work?

Many organizations have a DR plan and regularly test it, and the test fails. Then they have remediation plans, and they test it again, and it fails again. So asking “Does the DR plan do what it is supposed to do?” is perfectly acceptable. A cloud computing provider should be a specialist in the particular service they are offering.

Your Recovery Point Objective (RPO) in the case of a disaster should be real time or near real time. Recovery Time Objective (RTO) can vary depending on the needs of your organization and the likelihood of an actual disaster occurring.
Of course, understanding the resiliency of the cloud computing provider’s core infrastructure is actually more important than DR, but both are important. Loss of a particular system is likely and should have zero impact. Loss of a data center is, thankfully, a fairly rare event.

8. Do You Meet Critical Security and Compliance Requirements?

Getting answers to questions about security and compliance is a critical priority when evaluating cloud vendors. Cloud or not, your agency has to meet Federal Information Security Management (FISMA) requirements and remains accountable to regulators, other government organizations, citizens, and employees. You should only consider using cloud computing when the vendor has adopted a comprehensive and technically sound approach to a “defense-in-depth” security program. Make an effort to map your needs for security controls such as accountability, privacy, confidentiality, integrity, and availability to the vendor’s capabilities. Most agencies seek certification against the NIST 800-53 Moderate Controls.

- What are the vendor’s capabilities and policies in the protection of your data, both physically and procedurally?
- How is the application itself protected, and how is that protection maintained over time?
- How does the vendor meet general and industry-specific security and compliance standards such as Payment Card Industry Data Security Standards; Statement on Auditing Standards, Number 70 (SAS70); Health Insurance Portability and Accountability Act (HIPAA); NIST; and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). While you may be interested in only a subset of these, the breadth of compliance serves to indicate the strength of the cloud.
- How does the vendor meet your unique security requirements within your specific industry—in this case, government?

Security is a hot and sensitive topic, particularly when it comes to cloud computing. While real benefits abound, it is considered the #1 obstacle to cloud adoption across different industries, specifically government. The approach and technologies that a cloud computing provider uses to secure the cloud are likely similar to how an IT organization might go about securing their internal systems. It may not be the technology or procedures you need to question; rather, it may be how you will consume their security approach as a service. Compliance with various standards is another indication, as is the number of Authorities to Operate (ATOs).

9. Can I Simply Configure the Solution to Meet My Needs?

With large enterprise software applications, significant implementation services or projects are often required to meet the specific needs of a particular organization. Cloud-based solutions can provide much of this capability through configuration as opposed to custom code development.

In fact, one of the advantages of working with a cloud provider is that their economic model works best when they can provide a specific solution or service that fits the needs of most prospective organizations. Creating this capability is typically a focus of their engineering effort, so look to make
the system specific to your organization through configuration rather than customization. Look for features of the system that a technologist can configure—someone who is not a programmer but is tech savvy, understands systems, and can use built-in design tools to configure your implementation.

If the vendor wants to write a bunch of code to build your screens, workflow, and reports, your red flag is either that the solution is a bad fit for your organization or that the solution is inherently immature. Total configuration isn’t always possible, but for the basics look for advanced approaches such as drag-and-drop capability.

Some SaaS solution providers behave like traditional software companies by offering expensive customization instead of easy-to-understand configuration.

10. Do You Offer Robust Integration?

There’s really nothing you can do with on-premises software that you can’t do with a cloud computing model. At the end of the day, we all run our systems in data centers, and the fact that it’s in a remote location is really not unusual—whether it’s on premises or in the cloud. The potential gap is in what integration services are available to you. Less mature providers may not have had the opportunity to build out these more-advanced integration capabilities.

Understand not just the integration capabilities offered by a cloud application but the economics behind them. Sometimes the integration offering will have its own pay-per-use model, so be aware of the economic nuances of cloud integration and any imposing limits. It’s also important to ask a cloud vendor if their integration offering covers the breadth of capabilities you need in both the near and long term. The initial focus is often data integration, where information stored in back-office systems can be exchanged with the cloud service. However, if your goal is to consolidate the cloud solution into your master record management strategy, you may need an ongoing synchronization and not just an initial data seeding. If your objectives extend to automating the interaction workflow and visual component in the presentation layer of the cloud product, ask if the presentation layer also includes the extensible integration options that align with your objectives. This area is often initially overlooked, because data integration is the obvious primary focus. However, in the long run, the costs associated with the user experience are often where the greatest effectiveness and efficiencies are found.

A final important aspect of integration is integration and implementation resources, including third-party technology partners that have implemented turnkey solutions via the standard integration models. While open, standards-based integration technology is crucial, you also need to know that the vendor has a skilled pool of integration resources to call upon when needed. What internal professional services and systems integrator partner resources does the vendor offer?

Conclusion

As the need to balance greater citizen expectations with shrinking budgets intensifies, more organizations in the public sector are looking to technology to help. As a result, cloud computing adoption rates are increasing. However, many cloud vendors won’t be able to meet your high demands, so make sure every vendor you consider provides the answers you need to these 10 questions.
Ten Things to Ask Your Vendor Before Entering the Government Cloud

Updated May 2012
Author: Laef Olson
Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment.

Copyright © 2010, 2012, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0512

Hardware and Software, Engineered to Work Together