

# To Public Cloud or Not to Public Cloud?

5 Questions the C-Suite Wants Answered

# Executive Summary

**Companies that fail to tap the transformative power of the Public Cloud risk having circles run around them by those that do.** The decision to extend IT operations to a Public Cloud provider, however, is not one to be taken lightly. The C-suite wants answers on everything from how well a given application will perform in the Public Cloud to the overall cost effectiveness of migration.

Migrating infrastructure and applications to the Public Cloud requires tackling complex organizational issues.

**This white paper addresses five key questions to consider.**

**The Public Cloud has moved well beyond the hype stage.** Enterprises of varying shapes and sizes are experiencing the bottom-line benefits that result when users are able to outsource storage, computation and other services through a pay-as-you-go model. Upfront costs for hardware, software and IT are eliminated. Provisioning occurs in minutes instead of months. And innovation is fostered as new applications are rolled out with little investment and less concern about predicting outcomes.

But migrating infrastructure and applications to the Public Cloud requires tackling a host of complex organizational issues. Some are technical, while others require making a solid business case for the move.

**At the heart of it all is this fundamental question: To Public Cloud...or not to Public Cloud?**

## Question #1: "Are We Going to Save Money?"

The quick answer is "maybe."

**The logic is certainly sound: Massively scalable processing capabilities are delivered "as a service."** Organizations are able to shift at least a portion of their computing costs away from capital-intensive infrastructure to the more manageable operational expenses of a Public Cloud.

That said, cost savings are not a slam-dunk. An eyes-open cost-benefit analysis is required. Among the potential costs are:

**Data Transfer Costs** — There's a cost to moving all that data "across the wire." Public Cloud-based disaster recovery, for example, involves massive transfers of data as users continuously sync their Public Cloud and on-premises environments. Likewise, a bursting environment requires factoring in the cost of spinning additional resources during peak demand.

**Storage Costs** — Public Cloud storage costs are often a fraction of storing the data onsite. Yet eye-popping data growth could spell substantial lifecycle costs in the long run.

**Labor Costs** — Managing a large number of Public Cloud services is similar to managing a large number of onsite physical servers. Still, internal management costs of a Public Cloud environment are significantly offset simply by not having to provision (and replace) onsite servers — along with the overhead of system administration, facilities and disaster recovery. These costs are built in to the monthly fee for Public Cloud computing services and function as an operational expense.

### SO, IT ALL DEPENDS?

**Yes, there are inherent efficiencies in the Public Cloud model — but cost savings will ultimately be driven by how the technology is utilized.**

The problem occurs when you think of the Public Cloud as simply another layer of virtualization, says Ensono Solution Architect Jason Woodrum. "If nothing else changes and you try to use the Public Cloud in the same way you've used your existing infrastructure," he notes, "the costs savings are unlikely to materialize." That entails strategies such as leveraging auto-scaling and turning off/down environments dynamically.

### ASK THE QUESTION IN A DIFFERENT WAY

Like-for-like services in the Public Cloud come at a premium over traditionally delivered services. But that's not necessarily a bad thing. "It's important for organizations to focus on monetizing the Public Cloud," says

Cost savings are not a slam-dunk; an eyes-open cost-benefit analysis is required.



**Action:** Assess your current environment to determine the capacity that's needed all day, every day. Then determine how to solve any variability above that utilization level

Woodrum. “The question needs to change from, ‘Are we going to save money?’ to ‘Are we going to make money?’ in which case the answer is yes.”

An inherent challenge with current product development, Woodrum points out, is that valuable features are often delivered only after the competitive-advantage window has closed. This is where the Public Cloud is best leveraged. “The Public Cloud can help clients quickly prove a hypothesis, in the form of a minimal-viable product, and test their theory,” Woodrum notes. “This paradigm shift leads to making money, which is more positive than simply trying to save money.”

## Question #2: "What Application or Environments Should We Start With?"

**Truth is, not every app is a suitable candidate for the Public Cloud.** Legacy applications that run on unique hardware platforms may not be appropriate choices. Ditto for apps with very complex business processes that are specific to an organization.

That said, the increased resources offered by Public Cloud computing often lead to performance improvements. Automated scaling of resources in a Public Cloud environment can benefit applications that spread their workload across multiple servers. Public Cloud orchestration tools can be used to monitor and dynamically scale resources to match current demand without any human interaction.

Obviously, applications that were intended, or purpose-built, for the Public Cloud are a logical place to start. A lift-and-shift migration strategy might be more appropriate for legacy applications, as this approach requires minimal code changes. These applications are often already running on industry-standard stacks in a virtualized environment.

Companies are finding tremendous value in focusing on their core services, and reducing or re-focusing IT operations to the Public Cloud.

### LIFECYCLE CONSIDERATIONS

When considering Public Cloud candidates, The Public Cloud Standards Customer Council™ suggests evaluating where an application is in its overall lifecycle:

- Still being defined.
- Up for a refresh.
- Approaching retirement.

Based on your answers, look into whether the app can be redesigned or undergo a technology refresh for Public Cloud computing. Instead of migrating the existing application to Public Cloud computing, using an IaaS or PaaS approach, would it be better to replace it with a new SaaS solution?

If not, the Public Cloud may be an attractive option.

In terms of what environment to select, Amazon Web Services (AWS) recommends starting with a proven-concept environment, says Scott Millhollin, Product Manager for Ensono's Managed Public Cloud solution. "The idea is to turn on a few machines and deploy a duplicate database or duplicate SharePoint server that is not really in production," suggests Millhollin. "Put some data on it, and see how it runs and how your people manage the app. It's basically a crawl, walk, approach that minimizes risk and increases the likelihood of success."

## DETERMINE WHO'S COMFORTABLE WITH WHAT

**Start by determining your organization's readiness for Public Cloud computing.** Is the application owner comfortable with a Public Cloud platform? Is the corporate culture favorable to change? Is such a move within the company's risk tolerance level?

Next, assess the data. Determine the confidentiality, integrity and quality requirements of the data. Also look at how the application manages data requests from a safety and security perspective. Good candidates for the Public Cloud include apps with minimal customer data and other sensitive information.

Finally, select the most Public Cloud-ready application, taking into account these key considerations:

- Costs of migration and administration.
- Application redesign.
- Application performance and availability.
- Security and privacy requirements.
- Regulatory requirements.

## DIGGING INTO THE ONE-WISH PLAYBOOK

**If current companies were granted just one wish, it would probably be to start over with new Public Cloud-based applications.** Because this isn't a reality, many businesses find themselves trying to push up the stack in the opposite direction, says Ensono's Woodrum. "If a company is in some sort of managed hosting environment, it's just not feasible for them to say, 'Tomorrow, we're going to move our entire infrastructure to SaaS.' They have to move up the ladder in a methodical way. That means moving to an IaaS environment such as AWS, and then knowing they have the potential to move to PaaS and then SaaS."

Here, companies are well advised to start with lower-level environments, such as development, with the sole purpose of rebuilding their applications to be Public Cloud-native. At the rewrite stage, it's critical to focus on apps being



**Tip:** Think through the amount of data exchange that will occur between the components of the application and between the application and the user. Frequent data transfers may generate higher cost as well as performance lags.

Public Cloud Infrastructure-as-a-Service models are providing businesses the opportunity to modernize their application portfolios.

more modular. “That way you’re able to make changes to elements of an app without touching the entire app,” Woodrum shares. “So if I want to throw more horsepower at login, I can go through and make changes at that one microservice instead of having to rewrite the entire app.”

Just remember there’s no rush to move everything to the Public Cloud. Perform a thorough analysis of workloads. Consider what you’d like your IT staff to be focused on. Then use that as guide for mapping out how to best leverage Public Cloud computing.

## Question #3: "How Do We Keep Track of Our Resources?"

**Unlike managing a Windows or Linux server environment, the Public Cloud is dynamic.** Automatic provisioning and rapid elasticity mean that anyone in your organization can turn compute resources on and off, minute by minute. There can easily be several different accounts started by business units across the organization with a variety of resources provisioned.

### PAY-AS-YOU-GO MEANS TRACK-AS-YOU-GO

**Someone on the IT team will need to be in charge of tracking what’s running — and making the appropriate adjustments to over- or under-utilized services.** That includes shutting down ones that are no longer needed. If not, you run the risk of creating a graveyard of long-forgotten “zombie” apps.

Someone will also need to meter and track the spend. In particular, operating in a multi-Public Cloud environment means different bills, different products and different pricing. A team or teams should be charged with reviewing monthly invoices for accuracy and addressing any discrepancies. Obviously, accounting for these in the financial system becomes more complex when there’s a mix of OpEx- and CapEx-acquired services.

### MAKING CHARGEBACK (OR SHOWBACK) WORK

Given the Public Cloud’s radically different model of consumption, a chargeback model is a key requirement for ensuring governance and accountability.

The chargeback model can be a challenge for organizations that have not previously had to account for resource consumption. Processes will need to be created to inventory — and justify — each server and application as it’s moved to the Public Cloud. As an alternative, some organizations implement a showback process, where management can see where Public Cloud resources are being used, and then slowly migrate to a full-fledged chargeback model.

In the pay-as-you-go world of the Public Cloud, the meter is always running, making proper resource management critical.



**Tip:** Avoid sticker shock by establishing alerts that provide a heads-up when spending reaches a predetermined level.

## BEEF WELLINGTON AND RESOURCE MANAGEMENT

**Resource management becomes super critical on the Public Cloud, as every unused or underused resource represents money out the door.** Managing that complexity can be a challenge. “It’s like buying all the ingredients to make Beef Wellington, but not knowing how to boil water,” says Ensono’s Woodrum. Working with Public Cloud providers is similar. “They provide all the ingredients, such as API-driven interfaces for monitoring, reporting and tagging,” he notes. “So it’s easy to think that you can just lay all the ingredients out on the counter and make this incredible meal. The truth is that you may need the help of a master chef to put it all together. That’s where leveraging a service provider such as Ensono can help bridge the knowledge gap.”

## Question #4: "How Do We Secure the Environment?"

**Moving enterprise data and applications outside the firewall can feel like a huge leap of faith...and with good reason.** On a physical network, applications and data are separated and segmented. Networking, firewalls and security policies ensure it. By contrast, Public Cloud computing is a multi-tenancy environment that relies on shared resources. Virtual machines within a server are in constant, direct communication — sometimes across mixed levels of trust.

### A SHARED RESPONSIBILITY

Heavyweight Public Cloud providers such as Amazon Web Services and Microsoft Azure do their part with an army of full-time engineers and the deep pockets to keep one step ahead of security threats. As a user of the service, you need to deploy all the built-in security capabilities your Public Cloud service provider offers. Just make sure they’re in sync with your current security policy, and the processes and procedures you’re currently using. The goal is a consistent solution that ensures security is the same no matter where the application and data reside.

### HOW MUCH SECURITY DOES AWS REALLY PROVIDE?

In essence, AWS provides robust physical security and they secure from the virtualization layer down. “The virtual base software and the hardware that it runs on are all very secure,” shares Ensono’s Millhollin. “From a computing standpoint, they manage security up to the hypervisor. You are responsible for securing the operating system and applications. From a storage perspective, they provide the storage up to making it available for you to allocate, but they don’t encrypt it by default. They don’t manage the keys to do the encryption. You have to do that yourself.”



**Tip:** Identify latent security threats such as forgotten “zombie” apps, which present potential attack vectors.

Just remember that no Public Cloud provider is going to fully protect your data — that is ultimately on the user. At the system level, that means deploying tools such as intrusion prevention, application control, advanced anti-malware solutions and threat detection. At the application level, strong authentication tools should be deployed to protect apps against account credential hijack and authentication bypass breaches. Appropriate DDoS protection should be in place to ward off attacks.

“All of the ingredients for robust security are provided, but it’s your kitchen,” says Woodrum. “If you aren’t a good cook today, don’t expect the Public Cloud to solve this deficiency. This is where experts like Ensono can act as the sous chef, or head chef, depending on the company’s in-house expertise.”

Public Cloud application security involves a balancing act between business needs and security risks.

## Question #5: "How Do We Ensure Oversight and Governance?"

Just as the Public Cloud is a disruptive technology, so is it a potentially disruptive force in an organization’s governance strategy. Without sound governance, the risks include everything from Public Cloud sprawl and shadow IT to unauthorized Public Cloud activities that expose organizational risks.

“By moving an application to the Public Cloud, you introduce new risks that require new models of governance,” says Millhollin. “Traditional security and control processes designed for on-premise systems will probably need adjusted for the Public Cloud.”

It’s critical to note that bad processes will not become good processes simply by moving to the Public Cloud.

### CREATE A PUBLIC CLOUD GOVERNANCE POLICY

A good place to start is simply to determine who “owns” your Public Cloud. Who is accountable for the decisions, the architecture, the deployment and the operations? Then, address the expectations of the business users. There’s a delicate balancing act between providing the rapid provisioning and selfservice features the Public Cloud affords with the need for some degree of centralized control.

Given the incredibly dynamic nature of the Public Cloud, traditional governance processes — for example, those that require a very human signature for provisioning — may be too slow. Governance in the Public Cloud typically requires some sort of automation. (That might be a rules engine that leverages prescribed procedures for security levels and access without slowing things down.) Finally, tracking and logging all activities performed in the Public Cloud enable you to support audits and resolve incidents more quickly.



## A SHIFT IN CONTROL

Remember that as organizations move data to the Public Cloud, they relinquish some degree of control. Governance strategies must be structured to rely less on internal security and control, and more on their Public Cloud provider's offerings.

"Oversight and governance are the secret sauce of a service provider like Ensono," says Woodburn. "Clients are always fearful of 'losing control' when moving to a service provider, and the Public Cloud isn't any different. It's the partnership that is key. It's important to outline the structure of the engagement and partnership, establish a regular cadence for ongoing meetings, and collaborate on the appropriate artifacts. Because this isn't new to service providers like Ensono, it's a natural deliverable for us."

## FINAL QUESTION

With answers in hand, the final hurdle to Public Cloud adoption may simply be this: What is going to provide the confidence your organization needs to take that step forward?

"Something needs to make me feel confident that I can succeed," says Millhollin. "And that confidence comes from knowing I can do this in a logical, pragmatic kind of way that has clearly defined steps and low risk. I build some knowledge, perhaps utilizing a partner. I find a place to get my feet wet and maybe run it for a couple of months. Things are going well. I'm gaining documentation and understanding. Maybe I put a production environment out there or a test environment and I begin to leverage what the Public Cloud is really supposed to accomplish, which is to be a ubiquitous platform with infinite capacity that enables the business to succeed more quickly."

"Oversight and governance are the secret sauce of a service provider like Ensono."

-Jason Woodrum,  
Ensono Solution Architect

Ensono delivers complete hybrid IT services and governance from Cloud to Mainframe. Let us help you operate for today and optimize for tomorrow.

To learn more, visit [www.ensono.com](http://www.ensono.com).

