To Cloud or Not to Cloud

As the market and acquisition of cloud matures, informed consumers are recognizing that not every application or service belongs in the cloud, and no single cloud will necessarily meet all of an organization’s needs. The key is to zero in on the “what” — what services and applications are required and what are the measures of delivery success – without getting hung up on the “how” i.e. specific details on how the underlying infrastructure or technology is delivered.

Evaluating technology needs from an enterprise-wide standpoint will allow agencies insight into which technologies are appropriate, and how these technologies must interoperate to achieve the best end results. Vendors – whether or not they are cloud service providers (CSPs) – will have to build or modify their products to interoperate with as many technologies as possible, and remain technologically agnostic to best meet agencies’ changing needs.

Of course, agencies don’t have the luxury of building from scratch – they must start with what they have, set a course to meet their mission and business needs, and resist the urge to be driven by enticing new technology alone. Starting with an existing portfolio, an agency can quickly triage their holdings into several groupings, to understand where applications are best suited:

- Legacy systems and applications – evaluate for transformation or a shared service model
- Applications with sensitive information – evaluate security needs to consider on-premise or private cloud delivery
- Remaining services and application needs – evaluate for cloud suitability

APPLES-TO-APPLES COMPARISONS ARE NOT EASY

With a smaller pool of services and applications to evaluate for the cloud, a cost and fit assessment will help determine the best environment to realize efficient and cost-effective delivery. Several agencies are already realizing the benefits of this approach. For example, when the Recovery Accountability and Transparency Board decided to move to the cloud, they first determined which applications were appropriate for the cloud in general, then considered specific cloud environments for each application. The environment options include cloud platforms, co-location, managed hosting and on-premise. A full understanding of baseline costs as well as the total cost of ownership (TCO) for all of the available options is needed for agencies to make the most informed decisions.

The reality is that some agencies have not realized anticipated savings in the cloud because they encountered unexpected costs. Agencies simply did not know to adjust their baseline or were surprised by extra charges for services they thought were included. For example, if the baseline environment is not compliant with current Federal requirements, agencies may be surprised by the impact to pricing as a result of the additional costs and effort to achieve compliance.

It is also difficult to evaluate CSPs with the information that is publicly available. While the “pay-as-you-go” model seems to promise the lowest costs, agencies must be wary of hidden costs, such as services (e.g. patching, scanning, monitoring, etc.) that aren’t baked into the price, and extra risks such as CSPs who do not accept FAR (Federal
Acquisition Regulation) flow downs or charge an agency to take their data elsewhere. A trusted advisor or partner who understands delivery in the Federal market can help agencies develop apples-to-apples comparisons of CSPs based on their defined requirements.

**A WORD ABOUT SECURITY**

Federal agencies often raise security and privacy as top concerns, and organizations are finding that security is better and stronger in the cloud than in many legacy environments. Federal mandates, such as the Federal Risk and Authorization Management Program (FedRAMP), are standardizing and enforcing cloud security requirements. Agencies can take several specific actions to ensure security is firmly implanted into their cloud solution. First, they must clearly define requirements, put them into a compliance matrix, and use this matrix to guide the procurement from award to operations. Second, they should consider additional security controls such as data encryption and continuous diagnostics and mitigation (CDM). Security needs to be baked into architecture immediately, yielding a more secure environment at a lower cost.

**CRYSTAL BALL**

The future of cloud is bright – albeit complex. More hybrid-cloud solutions will appear, and the emergence and maturation of the cloud brokerage model will help agencies manage and move services as they seek the most efficient delivery. Many agencies will likely operate in an environment that utilizes the cloud in combination with on-premises and hybrid solutions. Rather than considering which specific infrastructure or individual cloud provider to adopt, Federal agencies may be better served envisioning a hybrid model for their enterprise – a model that potentially leverages multiple environments to efficiently meet business, security and system needs.

**LEVERAGE THE ENTIRE TOOLKIT**

Cloud is not a box to check or a goal to reach – it is one of many tools in the IT toolkit. The above blueprint helps agencies better understand the changing technology landscape within the Federal IT space. Organizations must carefully triage their existing portfolios to best determine which applications and services belong in which types of environments. Agencies must consider these guidelines in an innovative and well-thought-out manner to fully achieve cost savings and efficiencies.

**ABOUT CGI**

At CGI, we’re in the business of satisfying clients. As a global leader in IT and business processes services, our 68,000 members deliver end-to-end services and solutions in application and technology management, systems integration and consulting, business process management and services, advanced engineering and technology services, and operational support services. CGI was an early adopter of cloud technology and was the first large CSP to receive the FedRAMP Provisional Authority to Operate (P-ATO), as well as one of the first CSPs to receive the Defense Information Systems Agency’s (DISA) security accreditation. CGI’s Application Portfolio Management Framework (APMF) is a formal methodology and governance approach for the long-term management of application portfolios, based on a continuous improvement process.

To learn more, contact John Nemoto (John.Nemoto@cgifederal.com)