

Making the move to cloud-based ERP

Balancing the risks and rewards

More companies are looking to the cloud as a way to be more flexible and agile in their operations by accessing capabilities dynamically, and cloud-based enterprise resource planning systems are becoming part of their future plans.

As solutions for business needs go, the cloud is a whopper: a sort of grand, global smartphone, with an app for every need. In today's economy, where companies are constantly aiming for greater flexibility and efficiency, the cloud has emerged as a key strategy to not only reduce costs but also deliver business value through transformation of internal business operations, innovating around new products and services, engaging in new and diverse channels, and transforming IT organizations.¹

Cloud-based software as a service (SaaS) applications allow companies to transform their internal business operations and increase their operational performance by gaining access to process and technology capabilities that their on-site solutions have not been able to address. The increasingly fertile sector of cloud-based enterprise resource planning (ERP) allows you to pay only for what you use and avoid substantial investment in infrastructure, software, or personnel. It also allows access to information anytime, anywhere in the world, in a consistent format. For many businesses, this is a hard model to resist.

However, although the cloud is here to stay and adoption is inevitable, rushing rarely pays off. Instead, step back and develop a strategy for making the best use of this increasingly complex environment. You'll find that you need a different set of skills than the ones you use with an on-site system, one that will allow you to successfully adapt to the new era of working in the cloud. Consider these questions: Who's making the decision to move to the cloud? Will you realize the cost savings you expect? Which information should be in the cloud? Are you satisfied with the cloud provider's security controls? Are you able and prepared to change providers if you find a better solution? The clearer a company's understanding of the cloud's risks and rewards, the more likely it is that the company will realize the cloud's long-term benefits.

¹ "Looking at the Cloud through the Lens of Value," April 2012, *Forbes.com*

The cloud goes mainstream

The growth of cloud-based ERP

Today, the demand for cloud-based ERP systems comes mostly from small and mid-sized companies that are seeking cost savings and increased efficiencies. This demand has spurred the growth of technology companies that can provide SaaS offerings for the various aspects of accounting, human resources, manufacturing, customer relationship management, supply chain management, project management, and other business and IT processes.

The promise of simplified, cost-effective solutions has already resulted in a huge increase in the number of cloud-based system providers, as well as wider acceptance of cloud-based product offerings. According to Forrester Research, 25% of firms already have a centralized SaaS strategy in place, and others are moving to this model.² As cloud-based solutions become mainstream, we may begin to see larger companies replace or augment their legacy on-site ERP systems with less expensive cloud-based systems that can be deployed quickly and provide increased agility. Ingrained suspicions about the risks of having company information in the cloud should lessen as cloud providers adopt approaches to improve controls and transparency when reporting on their internal controls that address the security and data privacy and protection concerns of potential customers as well as

² Forrester Research, Inc., *The Benefits of Centralized SaaS Strategy* (October 18, 2011).

controls over the quality of information processing within a cloud-based ERP.³

Under the hood

Cloud-based applications run on an architecture that is highly flexible, scalable, and, most importantly, virtual. They are usually highly standardized solutions that offer only limited configurability — specifically because the cloud model is based on scale, and scale requires standardization. Their user interface is therefore highly intuitive, and the look and feel is consistent across applications.

Gaining initial access to a cloud-based ERP is straightforward: essentially, all you need to be up and running is an Internet connection and a valid email address. The time needed to deploy the product is four to six months, on average, and the cost for individual user licenses typically starts as low as \$2,000 per year. Depending on the number of users and the modules selected, higher-end small and medium enterprise customers are estimated to pay \$150,000 for license and support, which is significantly less than for an on-site solution.

³ To reassure customers that the risks of having their information in the cloud are mitigated, a number of cloud providers engage external firms to attest to their level of organizational control such as compliance with ISO 27001, PCI (payment card industry) standards, and issuing service organization control (SOC) reports.

All that's needed to access a cloud-based ERP system is an Internet connection and a valid email address.

The cloud goes mainstream

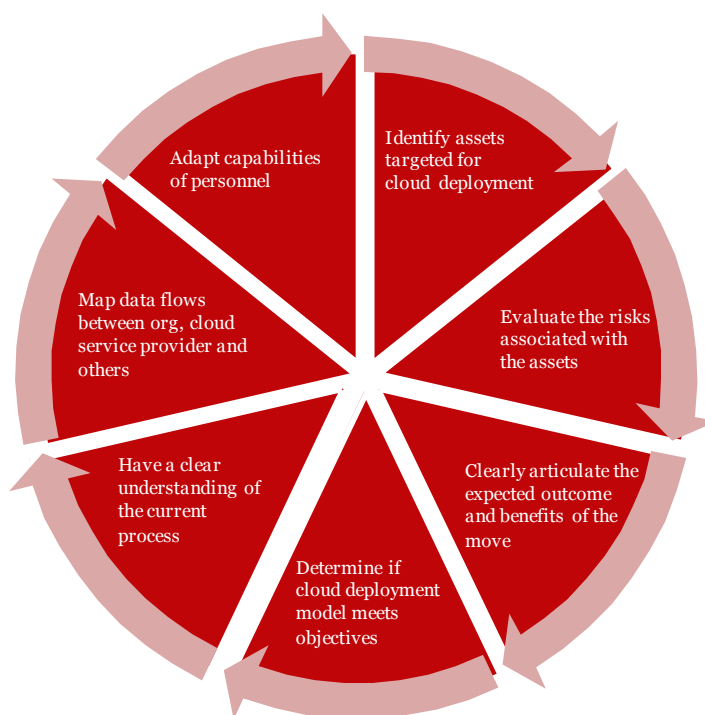
Cloudy with a chance of risk

Despite their advantages, cloud-based ERP product offerings also come with some known shortcomings, including the handling of newer revenue recognition rules, transfer pricing, international tax structures, and handling of inter-company transactions or consolidation. Because of these limitations, cloud-based ERP products do not currently appeal to many Fortune 1000 companies. Also, because ERP systems, whether cloud-based or not, are increasingly integral to the generation of corporate financial statements, it is important for them to be audited using a risk-based approach.

Companies that are considering moving their business processes to the cloud must carefully evaluate their goals and needs, understand both their current process and the risks, and be ready to provide ongoing management and oversight. According to a recent study, CxOs are now evaluating seven key considerations before moving their organizations to the cloud, as shown in Diagram 1. Considering these points carefully and having a knowledgeable internal audit function can help mitigate the risks associated with cloud shortcomings and also satisfy most auditing requirements related to financial reporting.

The following are additional areas where a robust risk management function can play an important role in protecting companies that choose to use a cloud-based ERP system.

Diagram 1: Seven key considerations prior to moving to a cloud-based model



The cloud goes mainstream

Application change management

One of the main characteristics of SaaS is standardization, with out-of-the-box functionality made available to companies quickly and economically, but usually in a way that is less specific to the business than would be the case with an on-site ERP system. One set of risks inherent in this model involves application change management, which is handled at least partially by the provider when bug fixes, maintenance requests, and code changes are released. These application releases are not specific to an individual account but are applied broadly over the entire hosted application's population. Most cloud providers will also introduce more substantial changes into the ERP environment. The introduction of such changes can significantly affect the way in which the data is structured and how it flows through the system, as well as how information is presented or reported. In a cloud-based environment, providers more commonly use an agile development model that makes small, repeated changes to the system, which improves overall performance but changes the functionality of the system in a way that makes it difficult for the user to track changes and assess which changes made "under the hood" could affect their business.

Without due diligence, proper reconciliation, and substantive testing, customers might overlook important changes to their environment. Some cloud providers also allow users to customize their

own system through the integration of APIs (application programming interfaces). Program changes made through APIs affect the source code of the system or, in the case of hosted applications, the individual virtual environment specific to a customer account. It is important that customers implement appropriate access and change management controls around APIs to ensure the integrity and appropriateness of the changes being made internally.

Third-party add-on software bundles

Another consideration is the emergence of application add-ons, known as "bundles." These bundles are software packages, developed by either the cloud provider or a third party, that reside on top of the cloud provider platform and serve as plug-ins to provide additional functionality and process automation. Customers using third-party bundles lack the assurance of a contractual relationship with their cloud provider, thereby putting their organizations at higher risk. Additional auditing and testing considerations can be used to boost customers' confidence in ERP systems that employ bundles.

Security management and virtualization

The security and integrity of customer data can be affected by a variety of risks. A client accesses a cloud-based application via the Internet, independently of its domain credentials or particular IP address, so protecting computer and

The cloud goes mainstream

mobile device browsers against security gaps is important in deploying a cloud-based ERP solution across the organization, as is the logical segregation of user accounts and data.

The use of virtualization by server administrators, whereby partitioned environments are created on individual servers, brings its own potential problems. While virtualization saves server and disk space by allowing multiple applications and customer accounts to run in parallel, it also raises security concerns about the commingling of data, super-user accounts, and hypervisor management, as well as the potential lack of security monitoring services that you would expect from physical network and security devices.

The end user also needs to be considered when an organization uses a cloud-based system. Access to programs and data through individual user accounts is the primary way for employees to manipulate and extract data. Standard IT controls, such as user provisioning, password enforcement, super-user account management, and periodic account reviews, can provide comfort around application access security.

Infrastructure complexities

The ambiguous nature of a cloud's infrastructure does not easily offer customers transparency about where their data is physically located. Organizations may be justified in assuming that their financial data is stored at the provider's primary

facility, for example, but many cloud providers sublease data center space in a co-location facility that is often operated and managed by vendors in other locations. The organization ultimately responsible for the physical security of the customer's data may in fact be a company with no formal arrangement with, or liability to, the customer.

These outsourced relationships, often referred to as "cloud brokerages," are not always evident to the customers. The responsibility for any problems encountered in key expectations about availability, performance, latency, security, or data protection may not contractually or legally rest with the contracted cloud ERP provider and may have been shared with or transferred to another cloud provider. Auditors of companies seeking to adopt cloud-based ERP services should therefore request and inspect an SSAE16 report from the provider, and also obtain and inspect a third-party assurance attestation report for any of the provider's subservice providers.

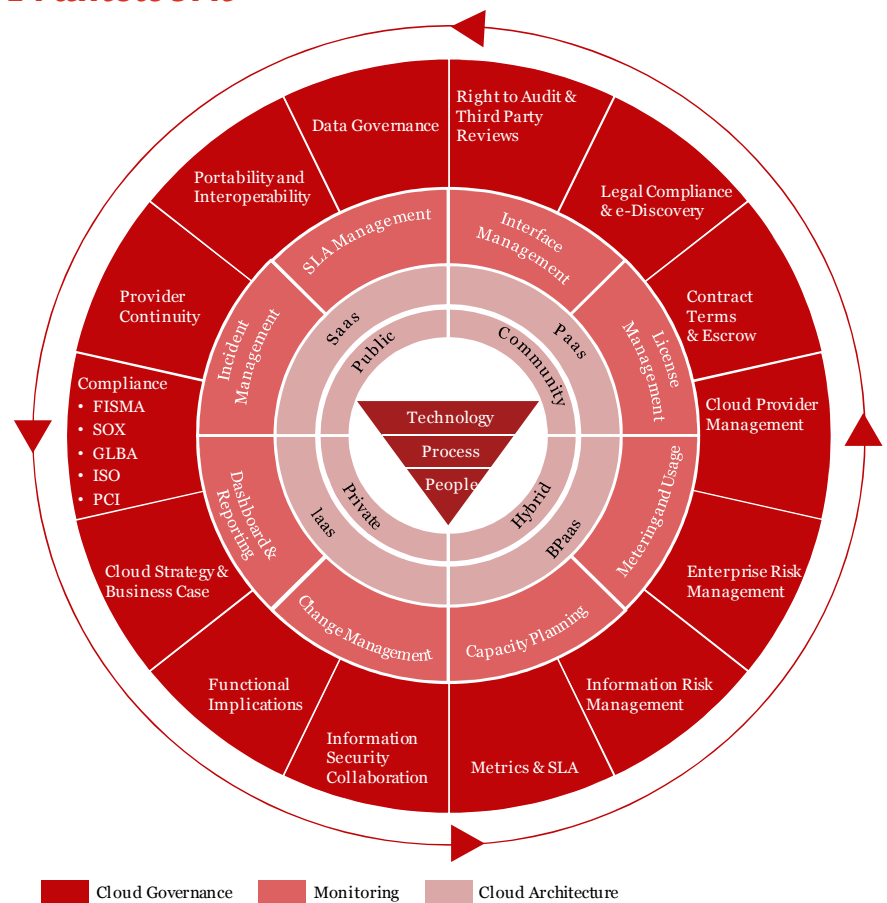
Similarly, organizations should be aware of any implications arising from changes in data privacy laws, tax codes, and information protection policies should the organization and the cloud provider (and any backup data center operated by the provider) be located in different states. The more locations and subservice providers used by cloud services providers, the greater the risk profile of their SaaS. For example, if a provider is backing up sensitive data in Massachusetts, it

will need to consider the requirements of the state's MA 201 data privacy law, which requires companies to have a program in place to protect the personally identifiable information of Massachusetts residents. Organizations need to focus on data classification as a key process before moving to the cloud: knowing what information they're moving, how critical it is, and what their obligations are.

Instilling confidence through risk management

Instilling confidence in a cloud ERP system that manages key operational and financial data needs to be an ongoing process, not just a one-time evaluation of the environment during procurement and due diligence. Unlike a software license, this is a long-term relationship in a service model where the vendor has significant control over the environment the organization uses to manage its business and financial processing and reporting. A company cannot gain confidence in the continued effectiveness of the system solely through periodic and cursory reviews of a report such as the traditional SSAE 16 (Reporting on Controls at a Service Organization) — partially because these reports do not address the risks and controls that many users of cloud-based services have today, which go well beyond the scope required for financial reporting. To address these issues, organizations relying on cloud-based applications need to maintain a sufficient level of internal control to provide reasonable assurance around risks such as privacy and security, processing integrity, and availability of the information and data in the cloud.

Diagram 2: PwC's Cloud Assurance Framework



Instilling confidence through risk management

Look before you leap

While similarities exist in the risks attached to both on-site and cloud-based ERP systems, the fact that cloud-hosting arrangements involve sharing IT resources with third parties, within an environment outside the corporate firewall, raises additional considerations.

Organizations must have a clear understanding of how the benefits of going with cloud-based ERP weigh against the associated risks, and how the anticipated cost savings and convenience of the cloud may be offset by the cost of guarding against those additional risks. Toward this end, PwC's Cloud Assurance Framework can help guide your organization in the right direction.

For additional information, you may contact:

Mike Pearl, US Cloud Computing
Leader, 408.817.3801,
michael.pearl@us.pwc.com

Cara Beston, US Cloud Assurance
Leader, 408.817.1210,
cara.m.beston@us.pwc.com

Eric Tan, Cloud Assurance Director,
408.817.7986,
eric.tan@us.pwc.com

Cornel Nolte, Cloud Applications
Leader, 408.817.5163,
cornel.nolte@us.pwc.com

Danielle Ritter, Cloud Assurance
Director, 408.817.3783,
danielle.ritter@us.pwc.com

© 2012 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms with 169,000 people in more than 158 countries. We're committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/us.