Moving your enterprise systems to the cloud? What do you need to know to manage the risks?

November 2015

Jamie Levitt, Director
Disclaimer

Certain matters reviewed today may represent services that PwC may be prohibited from providing to our audit clients. In those instances, the information is being provided to inform you of options that you may want to consider as you evaluate the solution described on today’s session. Due to the complexity of independence rules, any potential services for our audit clients should be discussed in advance within the context of the independence rules. The information contained in this document is provided 'as is', for general guidance on matters of interest only. PricewaterhouseCoopers is not herein engaged in rendering legal, accounting, tax, or other professional advice and services. Before making any decision or taking any action, you should consult a competent professional adviser.
Agenda

- Cloud and Cloud Solutions
- Workday
- Salesforce
- Key Takeaways
- Q&A
Cloud and Cloud Solutions
What is a Cloud Application?

A Cloud application is like a condo instead of a single family home. In a condo, you can paint the walls, add or remove furniture and even add or remove a door, but you can’t move a common wall or even change the tiles on the roof. The common walls and roof you share with other tenants is comparable to sharing the same line of code in a Cloud application. You can configure but you cannot customize. Some software vendors claim they are Cloud vendors in order to capitalize on market buzz. However, this is not always the case.
Cloud solutions

Demand for cloud computing is growing as services expand and awareness intensifies

Cloud computing is where shared resources and information are provided to devices on demand.

SaaS (Software as a Service) is a software delivery model where software is licensed on a subscription basis and hosted centrally (on the cloud).

Sample companies offering SaaS based solutions:
- Vend
- Intercom
- Twilio
- Zuora
- Hubspot
- Mulesoft

Gartner estimates that during 2015, 15 percent of business users are provisioned, in whole or in part, with office system capabilities from the cloud. Gartner expects this percentage to grow to around 60 percent by 2020.

Demand for Cloud is mounting: $150B Cloud market in 2015

-- Forrester Research, 2011

-- Gartner, 2015
Cloud Considerations

**Control**
Will we lose control moving to a hosted solution?

**Data**
Is my data safe? Will I be able to access my historical transactions?

**Flexibility**
Will the system fit our need / processes? How flexible is it really?

**Privacy**
Who else can see what we put in the cloud?

**Cost**
What is the cost to move? Will maintenance truly be lower over time?

**Availability**
Will my systems and data be available 24x7? How can I be sure?

**Reputation**
Do I run any reputational risks by introducing another party to my process?
**To Cloud or not to Cloud?**

As with any software selection, you should base your decision on a clear assessment of your needs and return on investment. Specific considerations should be given to the below cloud specific points:

- **Cloud is less customizable.** You cannot ‘lift and shift’ old legacy processes to a new Cloud application, the cloud processes will be less flexible and you will need to tailor your processes to fit. Do the cloud software’s processes fit your organization’s needs? Does your organization have the ability and willingness to change processes?

- **In many cases, the vendor is in charge.** You no longer control all access points to your data, the back ups and retention to that data, the controls possible in the system, or the availability of that data. You need to understand if you can live with what the vendor promises to deliver. You also need to acknowledge that issues caused by the vendor visible to the public may have a financial and reputational risk on your organization. Does the vendor offer independent attestations relating to it’s controls and processes? Are you happy with the rigor of those reports and who executed them? Do you have contractual recourse for things like availability issues or vendor-caused data leaks? In many cases, though control is relinquished, organizations conclude that a third party can manage these concerns better than they can in-house.

- **Implementation and on-going cost.** Once you move to the cloud it’s very difficult to move back without significant cost. Do you understand the on-going maintenance cost? Have you spoken to references to get comfortable that once you are onboard you won’t have significant cost increase? The number one reason organizations move to the cloud is cost reduction.

- **Cross border data.** Some geographical areas (like the EU) have very strict regulations on what can be viewed, stored, and processed outside it’s borders. You need to understand the implications of these types of restrictions as it relates to what you can put in the cloud.

We recommend that you prepare a solid business case, identify any areas in the organization that might resist process change, and understand what the cloud offers you and what it doesn’t.
## Cloud vs. traditional – comparison of solutions

**Benefits of shifting from traditional on-premise Enterprise systems to SaaS cloud solutions**

<table>
<thead>
<tr>
<th></th>
<th>Cloud</th>
<th>Traditional On-Premise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software</strong></td>
<td>Subscription</td>
<td>License</td>
</tr>
<tr>
<td><strong>Maintenance</strong></td>
<td>Included in subscription costs</td>
<td>Recurring annual license maintenance costs</td>
</tr>
<tr>
<td><strong>Time to implement</strong></td>
<td>Average 6 - 9 months, depending on scope</td>
<td>Average 1 to 3+ years, depending on scope</td>
</tr>
<tr>
<td><strong>Innovation</strong></td>
<td>Greater speed-to-market of new features and capabilities</td>
<td>Slower speed-to-market of new features and capabilities due to dependency on major releases</td>
</tr>
<tr>
<td><strong>Upgrades</strong></td>
<td>Upgrades/updates are managed by vendor with minimal effort required from client</td>
<td>Upgrades are based on major vendor releases with a high level of effort required from the client</td>
</tr>
</tbody>
</table>
| **Training / Change Management** | • Typically reduces training required due to more current user interface  
• Vendors typically provide ongoing training accessibility | • Depending on solution, may require more extensive training  
• Client is typically responsible for ongoing training, especially for custom business requirements |
| **Hardware**         | No additional hardware or install required  | Requires infrastructure impact assessment to determine need for new hardware, connectivity, etc. |
| **Main Suppliers**   | • Workday: Focuses on service-centric  
• NetSuite: Focuses on service-centric  
• Plex: Focuses primarily on manufacturing businesses | • SAP: Business Suite, Business By Design  
• Oracle: e-business suite, PeopleSoft, Fusion Applications |
Regardless the phase of the cloud journey you are in, you need to manage processes to meet external and internal compliance requirements through a reliable and sustainable internal control system.

**Which phase of cloud transformation are you in?**

**01**

Looking for a change

Will this change...?
- Impact compliance to external/internal regulations
- Impact the way you manage your financial data
- Impact your controls
- Impact the way users access to your data

Can you do it better....?
- Governance
- Process improvement leveraging cloud functionalities
- Integration with other systems
- Control optimization
- Security design

**02**

Going through a change

How are you...?
- Controlling the execution of your processes
- Managing compliance
- Managing the accesses to Clients data
- Creating efficiencies
- Integrating cloud app with other enterprise systems?

**03**

Up & Running

What are you doing to ...?
- Meet increasing regulatory requirements
- Get assurance over internal control system
- Maintain cloud apps in a controlled way
- Ensure the right level of governance over cloud apps

**04**

Continuous improvement

Can you do it better....?
- Governance
- Process improvement leveraging cloud functionalities
- Integration with other systems
- Control optimization
- Security design

Cloud

Regardless the phase of the cloud journey you are in, you need to manage processes to meet external and internal compliance requirements through a reliable and sustainable internal control system.
How to maintain ‘control’

Once you determine that cloud is the way forward, you need to define how you can control your new process and solution. This consist of performing the following steps:

1. Risk Assess Your To Be Process
   - Leverage your risk assessment from the software selection where possible. Ensure you understand all applicable regulations for the process.

2. Leverage Standard Controls
   - Review the standard controls available and supporting attestation reports / certifications to leverage as much as possible.

3. Configure Available Controls
   - For residual risks, where there are configurable controls available (such as access restrictions, workflows etc.) you need to design and implement configurations to mitigate risks.

4. Design Continuous Monitoring
   - Configurable and standard controls alone won't likely mitigate your risks. You will need to understand standard reports to define detective controls to mitigate risk. Where ever possible leverage dashboards to enable continuous monitoring for controls and to ensure your cloud solution is operating as intended.

Ensure controls are considered as part of contract negotiation so the organization has recourse for things outside their control.
Gartner predicts that by 2019, approximately 28 percent of installed human capital management systems globally will be SaaS-based, up from 13 percent in 2014.

-- Gartner, 2015
What is Workday?

More than just an HR system....
# Workday’s Standard Controls

## Workday offers...

- **ISO 27018 and 27001**
  - Information security

- **SOC 1**
  - Reports on Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting

- **SOC 2**
  - Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy

- **SOC 3 (SysTrust)**
  - Trust Services Report for Service Organization

## But don’t forget that...

- It does not cover information security of companies data managed outside the Workday cloud.

- You must read the SOC report to understand coverage!!

- SOC reports have a scope. You need to understand the specific controls covered as they are different for every report.
  - These reports also may have gaps / deficiencies.

- SOC reports do not cover financial controls for Workday configurable controls or interactions with other enterprise systems.
  - These reports do not cover end user control considerations. End user considerations together with the control activities at the service organization work in conjunction to achieve the related control objective.

- Companies need to specify which fields need to be encrypted.
## Workday’s Configurable Controls

Some example configurable controls for workday...

<table>
<thead>
<tr>
<th>Example risk</th>
<th>Workday controls</th>
<th>Workday benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payroll</strong></td>
<td>• Business process steps are configured to route transactions for approval if an payroll adjustment occurs.</td>
<td>• Workflow is standard, you are just configuring your approval strategy.</td>
</tr>
<tr>
<td></td>
<td>• Workday is configured to automatically populate payroll rates according to the business policies of the client.</td>
<td>• Standard calculations (i.e. Federal and Local tax rates) are automatically updated by Workday, thus can not be changed.</td>
</tr>
<tr>
<td><strong>Journal Entries</strong></td>
<td>• Workflow is configured to route all manual JEs for approval prior to posting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Non-standard journals are flagged for real-time review.</td>
<td>• Workflow is standard, you are just configuring your approval strategy.</td>
</tr>
<tr>
<td><strong>Segregation of Duties (SOD)</strong></td>
<td>• Workday comes with default SOD conflicts which can be configured to match your process. This allows for the system to flag users with a violation when an access request is made (i.e. before provisioning).</td>
<td>• Real-time reviews embed in the process reduce the overhead of manual reporting controls at periodic points.</td>
</tr>
<tr>
<td></td>
<td>• Analytics can be configured to automatically flag when a user performs conflicting actions.</td>
<td></td>
</tr>
</tbody>
</table>
## Workday’s Available Analytics

Analytics can provide coverage for areas outside of the financial transactions, including strategic, operational, and other compliance opportunities.

The use of analytics will be linked with risk and performance improvement use cases to provide:

- **Enhanced capabilities and re-usable analytics across risk areas**
- **Real time visibility to risk indicators**
- **Increased insight to transaction processing and compliance metrics**
- **Continuous monitoring of controls compliance**

<table>
<thead>
<tr>
<th>GL Close &amp; Journal Entry Analysis</th>
<th>Payroll</th>
<th>Accounts Payable</th>
<th>T&amp;E Expense</th>
<th>AR and Revenue</th>
<th>Fraud detection</th>
<th>Reconciliations</th>
<th>Continuous Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>(source, trending, user activity, unusual and common entries)</td>
<td>(payments before hire/after termination, high overtime, duplicate bank accounts, off cycle payments)</td>
<td>(duplicate vendor/payment, one time payments, trending of repeat payments, restricted vendors)</td>
<td>(whole dollar expenses, cash to credit ratio, miscellaneous/incompatible)</td>
<td>(customers without credit limit, duplicate customers, multiple credits, high volume activity)</td>
<td>Analyze manual journal entries for unusual combinations</td>
<td>Exception report of non-reconciling items between Workday GL and non-Workday sub-ledgers</td>
<td>Receipts Entered by Buyers, Indirect POs without Requisitions, Receipts Entered for Locations Other than User's location</td>
</tr>
</tbody>
</table>
Gartner predicts that by 2020, about a quarter of organizations in emerging regions will run their core CRM systems in the cloud, up from around 10 percent in 2012.

-- Gartner, 2015
What is Salesforce?

- Marketing Cloud
- Sales Cloud
- Service Cloud
- Community Cloud
- Other Apps

FAST APP DEVELOPMENT AND CUSTOMIZATION

SCALABLE METADATA PLATFORM

TRUSTED MULTITENANCY

API
Salesforce’s Standard Controls

Salesforce offers...

ISO 27001
Information security

SSAE 16/ISAE 3402 soc-1
Reports on Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting

SOC 2
Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy

SOC 3 (SysTrust)
Trust Services Report for Service Organization

But don’t forget that...

It does not cover information security of companies data managed outside SFDC cloud

SOC reports have a scope. You need to understand the specific controls covered as they are different for every report. These reports also may have gaps / deficiencies.

SOC reports do not cover financial controls for Workday configurable controls or interactions with other enterprise systems.

These reports do not cover end user control considerations. End user considerations together with the control activities at the service organization work in conjunction to achieve the related control objective.

It does not cover access by unauthorized individuals given by SF administrators

Companies need to specify which fields need to be encrypted. SF does not encrypt data by default
Some of Salesforce’s Key Control Considerations

Here are some of the common Salesforce risks that are overlooked during implementation and design:

• Change Management: Depending on the deployment method used by the companies, users may implement unauthorized changes directly into productions. For example, if the deployment of changes occurs via packages (instead of change sets), administrators may import a package directly into the production environment without testing it in a QA sandbox first (in salesforce all the environment different from prod are called sandbox).

• Security: Salesforce allows an administrator to log-in as a business user. This is a default setting that can be disabled. There are some workarounds to partially mitigate the risk (but not completely)

• Security: Security architecture in Salesforce allows users with a higher role in the organization to access data to all the users who report (directly or indirectly) to him/her.

• Sales Process: validation rules and approval sets should be set to automatically trigger the approval from the right level of management. Without this settings sales agents may apply non authorized prices or discounts.
Salesforce’s Controls

A. Business Process Controls
B. Access to Salesforce apps
C. Change Management and Salesforce App Development
D. Completeness and Accuracy of interfaces with other systems
E. Governance

salesforce App ecosystem
(2,400 apps)

analytics

Marketing Cloud
Sales Cloud
Service Cloud
Chatter

Salesforce1 platform
force.com
heroku

Compliance Essentials

Other systems

PwC
Key Takeaways
**Key Takeaways**

01. **Perform a fit-gap analysis** to determine whether going to a cloud based SAAS solution would yield an ROI for your organization.

02. **Assess risk areas** to identify new control requirements in adopting a new cloud based SAAS solution. Determine what areas are not covered with vendor’s certifications (i.e. SOC, ISO...)

03. **Optimize controls** available from the SAAS application during the initial implementation.

04. **Establish continuous monitoring** utilizing existing reporting functionality or leveraging a data visualization tool on top of the application’s analytics.
Questions?

Jamie Levitt
Director, Risk Assurance
Enterprise Systems Solutions
jamie@pwc.com
(949) 462-4592

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2015 PricewaterhouseCoopers LLP. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers LLP which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.