The power of Cloud
Are you truly a “digital utility”?
July 2020
Cloud Disruption

Many regulated electric, gas and water utility companies are planning their journey to become a truly “Digital Utility.” One of the most powerful, mature, and widely adopted technologies fueling that transformation is Cloud computing. However, unique regulatory and rate-making considerations native to the sector have historically created a bias in favor of on-premise solutions.

Cloud has evolved from a low-level technology cost arbitrage lever to a means for delivery model optimization, and now to a driver for business transformation through the delivery of rapid and flexible scalability, increased speed to market, and delivery of continuous innovation. As innovation continues to advance, what is today referred to as “Cloud” will likely be the way technology is architected.

Truly digital utilities that leverage the Cloud should be better positioned to cost-effectively process, analyze, and store vast amounts of data, and make use of artificial intelligence and other cognitive capacities like machine learning to better serve their communities’ needs. Cloud is rapidly becoming the preferred platform for foundational business applications such as enterprise reporting and for processing embedded sensor data such as information gathered from Smart Grid technologies or industrial control systems.

With this rapid evolution, coupled with evolving accounting and cyber considerations, now is the time to define a thoughtful and well-developed plan that extends beyond traditional IT implementation and sustainment activities to contemplate an organizational framework.

Accounting Guidance

Relatively recent changes in accounting guidance are opening new possibilities for the capitalization of certain Cloud computing costs. ASU 2018-15 (effective for public companies as of January 1, 2020) allows for the capitalization of Cloud computing or hosting arrangements which qualify as service contracts in similar fashion to implementation costs for internal-use software. Examples of implementation costs that may be capitalized under the new guidance as a prepaid asset include payroll and consultant costs directly associated with implementation and costs of software that allows for access or conversion of old data by new systems. Entities will need to work with their vendors to determine how best to identify the nature and cost of services provided. Consistent with prior guidance, costs of data conversion, training, and certain other costs must be expensed as incurred. Once implemented, ongoing Cloud costs continue to be expensed as incurred.

Some key provisions of the ASU include:

- The expense of ongoing Cloud service and the amortization of capitalized implementation cost of the arrangement are presented as a single line item in the statement of income.
- The balance sheet line item for capitalized implementation costs should be in the line item where a prepayment of hosting fees would be recorded.
- The cash flows related to capitalized implementation costs should be the same as the classification for fees related to the arrangement.

The adoption of the new accounting guidance can enable organizations to consistently capitalize costs to uniformly create assets that, in turn, can spread the impacts to operating and maintenance expense over a multi-year period (the life of the service contract), freeing organizations to select the technology that may have the greatest net benefit to the company and its customers.

Companies considering new investments in Cloud computing arrangements or changes to existing contracts should proactively address the following:

**Policies & procedures**

- Modernize and communicate a clear accounting policy that is easy to interpret, apply and govern.
- Build a consistent set of company-wide processes, tools, communication protocols, and organizational awareness methods for evaluating the accounting and regulatory considerations for Cloud computing arrangements.

**Contract optimization**

- Work with the supply organization to optimize Cloud computing arrangement contract terms and provisions to make clear what costs of the arrangement represent implementation costs.
Regulatory considerations

Under the new guidance, regulated utilities will enjoy uniformity of GAAP within the industry.

Regulated utilities are further impacted by the new accounting guidance given unique rate-making implications. Certain implementation costs associated with on-premise software solutions have been capitalized and earn a return on invested capital under the traditional revenue requirement formula for rate-making. In connection with the revised accounting literature referred to above, it is possible that a prepayment would not be reflected as a component of utility rate base and not earn a return on that similar amount of invested capital, albeit invested in a different form of software solution. Not earning a return on these amounts disadvantages the company comparatively.

In docket number AI20-1-000, the Federal Energy Regulatory Commission (“FERC”) provided guidance that Cloud computing implementation costs are similar to the costs incurred to develop internal-use software and should be classified as a utility plant asset and depreciated or amortized consistent with the requirements of the utility plant accounts in which the costs are recorded. This FERC guidance affords regulated utilities the ability to include Cloud computing implementation costs in a rate base calculation as a component of utility plant.

Further, individual states are recognizing the benefits of Cloud computing to their rate payers thus enabling Cloud computing costs to earn a return on investment. New York’s Reforming the Energy Vision program and Illinois’ proposal to allow 80% of Cloud hosting capacity and software subscription fees to be treated as regulatory assets are examples that underscore the need for utility companies to engage in an ongoing dialogue with their public service commissions to develop a thoughtful regulatory strategy.

Tax planning

As organizations consider Cloud, they must also pay attention to the impacts pertaining to the impacts of income and indirect tax rules to identify potential tax savings and help mitigate tax exposure. Tax compliance and planning factors to consider:

- Credits and incentives related to a Cloud transformation
- Review of transformation costs incurred to determine whether these should be capitalized or expensed for tax
- Analysis of cost-sharing arrangements pertaining to Cloud computing costs
- Understanding of which components of the Cloud computing arrangement are subject to sales tax, VAT and other indirect taxes

Cyber security considerations

Cyber is everywhere...

Cyber risks also need to be considered during an organization’s Cloud migration journey. Common challenges organizations face when migrating to the Cloud include:

- Complex regulatory environments make it difficult to keep up and maintain control over Cloud environments
- Cloud environments often lack automation to enable strong preventive controls that operate at the speed of business innovation
- Existing organizational governance models are not adequately designed to meet the demands of Cloud adoption and drive greater integration between the business and IT

Notable Cloud cyber risk trends

<table>
<thead>
<tr>
<th>Data protection</th>
<th>What does this mean for your organization?</th>
</tr>
</thead>
</table>
| As Cloud services become common, the risk of sensitive data being exposed increases | • Develop appropriate data classification schemas  
• Implement effective controls to protect data  
• Be aware of regulatory environment changes |

<table>
<thead>
<tr>
<th>Application security</th>
<th></th>
</tr>
</thead>
</table>
| Application development is outpacing organization’s ability to properly secure the data | • Incorporate security throughout development  
• Implement native or third-party security controls  
• Evaluate ability to comply with established controls |

<table>
<thead>
<tr>
<th>Infrastructure security</th>
<th></th>
</tr>
</thead>
</table>
| Increasing use of multi-Cloud environments results in control complexities | • Obtain visibility into services and assets deployed  
• Create secure default configurations  
• Automate provisioning of security controls |

<table>
<thead>
<tr>
<th>Resiliency</th>
<th></th>
</tr>
</thead>
</table>
| Increased use of Cloud to support the business is driving higher uptime, but 100% availability is not guaranteed | • Architect solutions for desired uptime  
• Monitor for Cloud denial of service attacks  
• Develop incident response plan for Cloud threats |
The power of Cloud | Are you truly a “digital utility”?

Data proliferation of confidential information in the Cloud may increase risk resulting in greater financial, brand, compliance and operational impacts. To help address these challenges, organizations need to understand that the Cloud security landscape requires well-defined, joint responsibility between the enterprise and the Cloud provider. Security in the Cloud is the organization’s responsibility while security of the Cloud is the Cloud provider’s responsibility.

From a sector perspective, compliance with North American Electric Reliability Corporation’s Critical Infrastructure Protection (NERC-CIP) standards must also be taken into consideration when evaluating Cloud solutions. Presently, certain systems and associated data are not positioned for full Cloud adoption under existing NERC standards and requirements. However, in 2019, a Standards Authorization Request was filed to continue NERC’s effort to modify the requirements to enable virtualization capabilities. There are several changes that will be required to address challenges unique to virtualized environments for compliance with the CIP Standards. This includes areas such as asset classification, access control, firewalls, storage, encryption key management, and more. As companies work to address these challenges, there is still opportunity in the near-term to explore hybrid Cloud/On-Premise solutions, as well as designing longer-term roadmaps that can pave the way for a broader march toward Cloud adoption once the necessary modifications to the NERC requirements are put into effect.

The future is here, prepare now

Cloud computing is here to stay. Technology decisions are no longer solely the domain of your IT department. Now is the time to assess and understand the organizational impacts from the accounting, regulatory, tax, and cyber perspectives to prepare the organization to broadly adopt Cloud technology in order to achieve the desired benefits and reduce risks.

Authors:

Bill Graf
Partner
Deloitte & Touche LLP
US Power & Utilities Audit & Assurance Leader
wgraf@deloitte.com

Katie Pavlovsky
Principal
Deloitte Financial Advisory Services, LLP
US Power & Utilities Risk & Financial Advisory Leader
kpavlovsky@deloitte.com

Dave Yankee
Managing Director
Deloitte Tax LLP
US Power & Utilities Tax Leader
dyankee@deloitte.com