

STATE OF ILLINOIS

ILLINOIS COMMERCE COMMISSION

Illinois Commerce Commission	:	
On Its Own Motion	:	
	:	16-NOI-01
Notice of Inquiry regarding utility	:	
adoption of cloud-based solutions	:	

INITIAL COMMENTS OF COMMONWEALTH EDISON COMPANY

Commonwealth Edison Company (“ComEd”) submits these initial comments in response to the Illinois Commerce Commission’s (“ICC”) Notice of Inquiry (“NOI”).

Cloud computing hosting solutions can be implemented in many different ways. There are a variety of reasons and supporting analytics for implementing the options offered. In its comments, ComEd offers a high level overview of the various types of cloud support options and the general evaluation criteria to assist with making a choice. Companies evaluating systems continue to compare on-premise solutions with cloud solutions to ensure they have entertained the robust arguments for both options in order to select a balanced approach which considers both the technology and ultimate cost. There are four key solutions when evaluating systems:

- Software as a Service (“SAAS”) – Software applications reside with a provider or developer and user access is provided thru a web interface. The provider or developer of the software provides all services for the application such as hardware refresh, system patching and application enhancements and upgrades. The end user has the ability to use the system but is not granted authority to make changes to the system. The benefit of SAAS is that the client does not have to create the application; however that can result in limited customization for client needs.
- Platform as a Service (“PAAS”) – With PAAS, an environment (hardware and software) is hosted and maintained by a vendor that clients use to develop and run applications. PAAS provides the set of tools and services designed to make coding and deploying those applications quick and efficient with no requirement for the client to maintain the infrastructure themselves. The primary benefit of PAAS is quick access to development environments which minimize the time required to build an application.
- Infrastructure as a Service (“IAAS”) – Choosing an IAAS solution allows a client the flexibility to use servers, storage, networks, operating systems – the hardware and software that powers it all – without the up-front cost to purchase the infrastructure or the ongoing maintenance burden.

- On-Premise – The solution is installed and operated on hardware on the premises (in the building) of the organization using the software, rather than at a remote facility.

Evaluation criteria should include items such as data throughput, latency, connectivity, security, compliance requirements (i.e. can data be moved off site or off country), costs, and capitalization.

In the utility industry, applications have traditionally been hosted on-premise due to lack of cloud offerings, security and privacy concerns, and connectivity models. With the advances made in cloud computing and the multitude of offerings available in the cloud, utilities evaluate each situation on balance to determine when the cloud proves the better choice. Trends are emerging which help drive decisions between cloud hosting versus on-premise, including the following:

- 1) New System Implementation - When there is no existing system, and hardware and software would have to be purchased, programmed, configured and maintained for an on-premise system, the benefit of using a cloud provider may outweigh creating an on-premise solution, especially when a standard solution exists in the cloud.
- 2) System upgrade – When an existing system requires lifecycle refresh or application enhancements, and the connectivity and interfaces for the system are already in place, the costs of moving the system to the cloud may be cost prohibitive. Considerations include costs and payback periods, connectivity, security, compliance requirements and timing, vendor support of products and change management.
- 3) Variable needs – When there is a need for dynamic processing power or storage, the cloud generally offers solutions that can meet these variable needs more quickly and efficiently than traditional on-premise solutions. In addition, cloud computing offers the flexibility of only paying for what you need, when you need it. With on-premise solutions, the maximum hardware and storage must be purchased to meet the maximum needs, thus costs are committed regardless of whether they are continuously used.

Cloud vs. On-Premise IT Solutions

A. Cost:

1. *Identify how costs differ between a traditional on-premise IT system and a cloud-based solution, including all relevant costs and timing of costs.*

Costs between these two solutions depend on many factors. A key consideration in choosing a solution is the strategy of the company; whether they want to be operators of assets owned internally thus maintaining more control, or operators of assets owned by an external provider thus maintaining more

efficiency and agility. The cloud service model (IaaS, PaaS, SaaS) chosen for each solution will dictate what is managed by the individual company as opposed to the Cloud Service Provider (“CSP”). ComEd’s experience (supported by many IT strategists) is that the current economical and operational balanced scorecard lies in SaaS and PaaS adoption as opposed to IaaS because they allow for more efficiency and agility with solutions as new technologies are emerging. The table below reflects the spectrum of control and flexibility versus efficiency and agility based on each individual solution.

TABLE I



Generally the cost model employed by CSPs for cloud solutions is often referred to as an OPEX model. It is generally a consumption-based, pay-as-you-go model where a company can start or stop using a product or service at any time thus avoiding long-term contracts.

As implied by the same table, with solutions where a company typically owns and manages the assets, that company incurs all costs for the life of asset, whether it is used or not. This is often referred to as a CAPEX model, based on the utilization of up-front capital dollars (which involves depreciation costs).

Generally companies choose cloud based solutions primarily based on operational factors such as agility, innovation and managed services. Cost is often a secondary consideration as cloud solutions are not always less expensive than on-premise solutions.

2. *Describe the costs associated with migrating utility data systems to cloud services. What evidence have stakeholders seen of this shift and what are the results? How long would it take to migrate utility data from on-premise IT to a cloud solution? Provide examples of utility services that have migrated from utility-owned systems to cloud services.*

As stated in response to Question 1 above, ComEd's experience (supported by many IT strategists) is that the current economical and operational balanced scorecard lies in SaaS and PaaS adoption as opposed to IaaS. Costs associated with migrating utility data systems to cloud services include:

- **Infrastructure Costs (applies more to IaaS model):** Infrastructure and resource costs in cloud environments tend to be lower (per machine, per gigabyte, etc.) than traditional on-premises infrastructure. This is primarily driven by economies of scale since cloud environments leverage millions of virtual machines and exabytes of data to drive costs down. Prices continue to drop and be adjusted many times throughout a given year.
- **Governance and process costs:** Choosing a Cloud based solution requires a commitment to review the processes of the CSP - e.g. from legal, security, compliance, financial, architecture, and operational viewpoints.
- **Integration costs (with other systems – typically on-premise solutions):** Integrating the cloud based solution with other on-premise solutions is often necessary - e.g. identity management/security, application and data exchanges.
- **Operational costs:** Depending on the level of control and ownership of the solution, operational costs such as continued monitoring, support, patch and upgrade costs will be incurred.
- **Network connectivity:** Charges apply where a direct/private connection to a CSP is required or desired.
- **Training:** Training of IT personnel for management, support, and integration of cloud based solutions as well as for users of the software/platform.

Migration plans must include the size of the data, the bandwidth of the connectivity to the CSP and the physical proximity between the company and the CSP. The time to migrate the data will depend on all of these factors.

Examples of utility services that have migrated from utility-owned systems to cloud services include:

- Smart Meter back office system used to obtain data from smart meters is hosted at Silver Springs under a SAAS model

- iFactor (<http://www.ifactorinc.com>): iFactor provides outage and work order maps
- Navigant Evaluation Services: Navigant provides for evaluation of ComEd's Smart Ideas incentive programs
- Agent 511 Preference Center (<http://www.agent511.com/utility.php>): Captures customers preferences, processes the preference data through a rules engine for notification, and allows us to communicate with our customers based on their communication preferences
- Opower (<http://opower.com/>): Opower web portal software provides customers with better information about their energy consumption, along with personalized ways to save energy and money
- AMI - Energy Insights (<https://www.comed.com/business-savings/energy-tools/Pages/energy-insights-online.aspx>): Energy Insights Online monitors your electricity consumption via special recording meters and converts this data into simple, easy-to-understand usage graphs and reports that you can access online.
- CRM (Customer Relationship Manager) tools are being offered as cloud solutions. A few examples include Microsoft (Dynamics) CRM (<https://www.microsoft.com/en-us/dynamics/crm.aspx>) which is being used in Commercial, specifically Retail and BGE Home; ComEd uses a cloud solution called SARATOGA CRM as well.
- Microsoft Sharepoint Online: This solution is leveraged as a basic content management system to present some customer/business partner web sites.

3. *Identify costs associated with training employees to use cloud-based solutions and whether those costs differ substantially from costs to train employees to use utility-owned, on-premise systems.*

As depicted in TABLE I above, the level of direct management of the cloud service decreases as one moves across the spectrum of IaaS to SaaS models; thus, training and associated costs should be relative. Cloud deployments do not vastly differ from on-premises deployments, however, and there are some key differences on which users must be trained (e.g. in cloud terminology, architecture and constructs). When moving to cloud environments, utilities will see an initial increase in training costs, to ensure IT professionals understand how to deploy to the cloud, how to migrate services to the cloud, and what the key differences are between traditional IT deployments and cloud deployments. From an end user perspective, training costs for cloud-based solutions should be relatively flat or lower than traditional on-premise solutions as most cloud based solutions are more thoroughly documented, publicly available, provide online learning, and have more intuitive interfaces.

4. *Describe whether and how operations and maintenance costs differ between utility-owned, on-premise systems and cloud services.*

Operations and maintenance costs generally decrease as one moves across the spectrum from IaaS to SaaS models. ComEd has found O&M support costs for IaaS solutions to be the same or higher than on-premise solutions as cloud resources require similar support resources (e.g. data management, monitoring, patching, software, incident and problem resolution). In addition, cloud based solutions may include additional charges such as support plan charges and private network connectivity charges, among others. Finally, state and local “cloud taxes” should be considered when looking at operations and maintenance costs.

B. **Reliability:**

1. *Describe whether and how cloud-based solutions improve safety and reliability at a utility.*

The safety and reliability of a utility’s infrastructure largely depends on infrastructure, culture, and processes. The impact of a cloud based solution on a utility’s safety and reliability is largely dependent on a given utility’s IT availability, data reliability practices and security rigor and maturity. For example, access to outage maps or restoration time of automated functions will help with reliability, however systems are built with business continuity plans offering manual options in emergency situations. Further it depends on the specific cloud based solution and its architecture. ComEd’s response to Question 2 above lists some examples of cloud based solutions that can enhance reliability such as the iFactor outage maps.

The Microsoft Azure cloud computing platform is one example of a solution that impacts reliability and security. Key considerations include:

- **Uptime and Availability:** Cloud environments could enhance a customer’s uptime (the time a computer can be left unattended without crashing) and availability posture. For example: Azure provides 99.9% financially-backed uptime guarantee for cloud services. Azure also has 22 regions worldwide, which hold up to 16 datacenters each. This provides broad scale and global availability. Certain services like Azure storage have multiple copies of data to ensure continuous availability. That said, applications built on these services can be architected to have even higher availability, depending on need.
- In addition to high availability and disaster recovery scenarios within the cloud itself, Azure also provides robust ways for customers to failover existing, on-premise applications into Azure. This may provide a cheaper, reliable alternative to a standard Direct Current-to-Direct Current replication.

- **Security and Compliance:** Azure meets a very broad set of international and industry-specific compliance standards, such as ISO 27001, PCI, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country/region-specific standards like Australia IRAP, UK G-Cloud, and Singapore MTCS, EU Model Clauses, amongst others. Rigorous third-party audits, such as by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. The Azure Government cloud provides the highest level of security and compliance for government (and supporting) agencies like DoD, FBI, DOHS, etc. This commitment to the highest levels of security, privacy, and compliance makes it easier for customers to lock down their data while compliance with a wide array of industry regulations.

2. *Proven Cloud Technologies in Regulated Utilities*

- Identify the cloud services that have proven most successful for public utilities. Identify the differences between a public versus a private cloud, and determine whether one is more appropriate for the utility industry.*

Cloud services that have proven most successful for public utilities thus far include solutions for outage and restoration time maps, demand management services, communications services, and work management applications. Some of these solutions were discussed in ComEd's response to Question 2 above.

A private cloud hosting solution resides on a company's intranet or hosted data center where the company's data is protected behind a firewall. This can be a great option for companies who already invested in expensive data centers because they can use their current infrastructure, they likely have an increased level of security and they do not typically share resources with other organizations. Challenges with a private cloud are that management, maintenance and updating of data centers is the responsibility of the company and it is expected that over time hardware and servers will need to be replaced adding additional cost.

The main differentiator between public and private clouds is that the management of a public cloud hosting solution is performed by the CSP. This type of cloud environment is appealing to many companies because it reduces lead times in testing and deploying new products. However, many companies feel security is not as robust in a public cloud environment.

When determining the right environment for a utility, the key consideration is control. The utility must decide how much they want to own, maintain and control the environment.

- ii. *Identify public utilities that have adopted cloud-based solutions and what effect cloud services has had on the utility's safety and reliability.*

Utilities in general have so far adopted a more limited set of cloud services than have other industries, instead tending to focus on the particular applications identified above. Cloud is emerging in back office applications however it is not yet prevalent in the operational space. Microsoft discusses a few customer success stories such as virus protection at American Water and customer service and relationship management tools emerging internationally at the following site:

<https://customers.microsoft.com/Pages/advancedsearch.aspx?-mrmcverticals=Power & Utilities>

- iii. *Identify circumstances where the utility and its customers are better served by a combination of utility-owned, on-premise IT systems and cloud services, a "hybrid" model. What approach best maximizes reliability, safety and security for a utility and its customers?*

There are many examples of hybrid solutions in use across the utility industry. Most of these solutions have cloud systems integrated with on-premise systems in order to share data and to send commands back and forth. A prime example includes ComEd's metering systems. Back office functions such as meter reading operates in the cloud. Meter reads are then sent to an on-premise meter data management solution, which performs billing functions and shares the data with the customer billing system. In this situation, the external provider cannot perform every aspect of the meter to cash cycle, thus we have leveraged interfaces with existing systems giving us a best in class solution. Currently, ComEd is not aware of a vendor that offers a robust end to end meter to cash solution, thus a hybrid solution was the only option.

The best approach to maximize reliability, safety and security will be situation dependent. A solution may have components with differing requirements that are better served by on-premise solutions versus cloud solutions or vice versa.

3. *Identify successful cloud services adopted by non-utility, but highly regulated, companies or industries. Explain any lessons from their experience that can help maximize reliability, safety, and security for a utility and its customers.*

There has been significant Cloud services penetration across different industry groups as companies seek to reduce total IT lifecycle costs, closely

align with company strategic imperatives, enhance cyber security, and enable more rapid deployment of new capabilities to address industry trends. Below are two specific examples of successful cloud services adopted by non-utility, high regulated industries:

- 1) **Banking industry** – as the industry faces ongoing pressure to reduce costs of its core operations, protect confidential customer information, meet the evolving needs of customers, and disruption from low cost on-line competitors, an increasing number of banks have been cleared by regulators to use cloud services for a range of banking services including websites, mobile applications, retail banking platforms, high performance computing and credit risk analysis. These companies have seen banks improve their effectiveness in areas such as security, and new products and services introduction, particularly in light of recent requirements where regulators are requiring higher bank capital levels and through migration to the cloud can reduce capital expenditures and re-direct to other needs.
- 2) **Insurance industry** – Insurance companies have been looking to cloud services to help mitigate impacts from non-traditional competitors, increased frequency of catastrophic events, and the need to manage risk more accurately. In addition to utilizing the cloud as a proxy for traditional IT infrastructure and platform needs, insurance companies are now using cloud solutions for core insurance activities such as claims first notice loss, billing, and extended distribution channels. These insurance companies have seen some important lessons learned as they began their cloud computing journey addressing back-office functions, and now are evolving to more front-office needs such as harvesting real-time data in the field in order to more accurately gauge risk.

C. **Cybersecurity:**

1. *Cloud Security*

- i. *Describe whether and how utilities will benefit from the cybersecurity practices provided by cloud-based solutions providers versus those associated with on-premise solutions.*

Cloud based solutions offer very large scale systems and include intrinsic resistance and resilience to security events, providing a direct benefit to a utility's security posture. Cloud providers deploy automated systems to deliver software and operating system updates and patches to ensure that these critical processes are executed in a timely and accurate manner. Further, Cloud solutions are typically more dynamic and agile and can be provisioned and scaled up or scaled down as needed via automated processes or light administrative tasks. Utilities

can harden their systems by leveraging economies of scale with cloud solutions providing a direct financial benefit and enhancing the utility's security posture. Finally, utilizing cloud providers ensures that data is stored in the Cloud, not on a user laptop or mobile device, enhancing confidentiality, reducing the attack surface, and reducing risk of unauthorized data disclosure. Storing data in the cloud also ensures it can be accessed irrespective of what happens to a particular end user device.

On-premise solutions have the benefit of direct oversight and control of the systems. Exact understanding of the architecture of all components and connections (which you get with on-premise) allows a greater understanding of security and evaluation of risks. It can be difficult to obtain security details from external vendors unless this expectation has been specifically laid out in a contract requirement. Also if there is a security breach the systems can be isolated at the exact point to allow isolation of the issue but maximum connectivity, which may be more complicated with a cloud solution where a complete disconnect could be required.

- ii. *Identify any cybersecurity benefits of using a cloud-based solution versus an on-premise IT system.*

Using a cloud provider can generally enhance the hardening of a solution as it can reduce the potential attack surface, provide redundancy and quicker response time and can be less expensive. When solutions or services are deployed in a Cloud provider's environment, any attack against those solutions or services are directed toward the cloud provider's data center or infrastructure, thus the threat is contained and not targeted to one individual company. In addition, Cloud providers offer redundant IT resources as well as quick failover mechanisms in the event of a failure of any given server or component. This can benefit a utility directly since the hosted applications and services can easily be transitioned to other servers or hosts within the Cloud provider's enterprise. Finally, larger providers including Microsoft, Amazon, and Oracle are members of the Cloud Security Alliance, which maintains standard security requirements across providers resulting in consistency and accountability for those in the Alliance.

These economies of scale, redundant systems and quick response are generally harder to achieve and more costly with regard to on-premise solutions.

2. *New Risks*

- i. *Describe the extent of new risks introduced (if any) when a utility migrates to a cloud-based solution from an existing on-premise system.*

Cloud service providers are generally required to implement very stringent utility approved security standards and controls based on the sensitivity of the underlying data and the specific requirements of any given solution. The ease in procuring and accessing cloud services can give nefarious users the ability to scan, identify and exploit loopholes and vulnerabilities within a system. For instance, in a multi-tenant cloud architecture where multiple users are hosted on the same server, a hacker might try to break into the data of other users hosted and stored on the same server.

In addition there are some lower level risk items such as the inherent technology risk due to loss of control of the data when it is stored outside of a utility's premise. Internal risk and security assessment processes are critical to ensure that any Cloud provider who will be storing any utility data has been thoroughly vetted, has achieved appropriate industry certifications, and can provide the necessary security controls for storing data and important files. In addition, legal hold and regulatory audit requirements must be considered when storing data in the Cloud.

3. *Incident Response*

- i. *Describe how cloud-based solution providers can respond to cybersecurity threats in contrast to utilities utilizing on-premise systems.*

Cloud-based solution providers utilize automated systems to deliver software and operating system updates and patches, reducing time to deploy these critical security updates from days or weeks to minutes. When such updates are applied to an on-premise environment, significant testing and quality control measures must be performed prior to deployment. Further, Cloud based solutions offer very large scale systems and includes intrinsic resistance and resilience to security events. Finally, most utilities require Cloud service providers to have a published and approved security incident response plan that specifies how the Cloud service provider will detect and respond to security incidents, and includes a requirement for a cohesive Communication Plan for the utility owner of the data. A Security Incident and Event Management (SIEM) data feed to a utility's Network Operations Center is also typically required.

4. Threat Detection

- i. *Describe whether and how a cloud-based solution can assist a utility in protecting, detecting, and responding to cybersecurity threats and operational vulnerabilities.*

Typically, cloud-based solutions are more agile, allow for quick analyses of large amounts of data and include robust incident response plans. Cloud-based solutions can be more flexible, available, and resilient than on-premise solutions. Large scale, Cloud-based assets can be migrated easily in the event of malicious attacks exploiting cyber focused vulnerabilities, or a penetration attack which targets a particular host, subnet, or physical data center. Further, the Cloud-solution provider's large scale infrastructure, coupled with the large internet presence required to provide effective Cloud services, allows the Cloud provider's NOC and Incident Response teams to analyze large amounts of data in real time from many hosts, load balancers, routers, and other IT systems, etc., to detect and respond to malicious attacks and anomalous events.

Finally, an intrinsic capability of a Cloud-based solution is the ability to activate a utility approved and directed Incident Response plan, which would empower the Cloud provider to transparently and seamlessly move the vital services or solution components to hardened, patched Virtual Machine hosts, in a different physical data center if necessary, which are not vulnerable to the attack. If a cybersecurity event is in progress, and the Cloud-based provider is under direct attack, the Virtual Machines, circuits, routers, firewalls, etc., can simply "drop" the affected / under attack Virtual Machines and other infrastructure components, having already moved and migrated the services or solutions to other hardened Virtual Machines elsewhere within the providers cloud.

5. Security Framework for Utilities

- i. *Identify the key elements and value of a security best-practices framework for utilities to address cybersecurity threats.*

The key elements of a "best-practices" framework are the structured taxonomy of defining security requirements, security controls, and regulatory compliance controls to act as a model for the utility's security policies, practices, and procedures.

- ii. *Identify the security best-practices framework you would recommend for Commission adoption and explain why.*

ComEd recommends utilizing the ISO/IEC 27000 Series as the overall Information Security structure, and implementing the necessary corresponding security controls as defined by the NIST specifications.

The ISO/IEC 27000 series of published Information Technology and Information Security documents provide scope, normative references, and security control objectives to act as a model and set of guidelines for complex enterprises. Current updated documents in the ISO/IEC 27000 thru 27018 series provide for protection of personally identifiable information (PII), and define controls for Cloud privacy. The ISO/IEC series defines Security Control Objectives (i.e., encrypt data), but does not define the exact security control required (i.e., encrypt data utilizing AES 256 XTS Mode).

Current NIST Information Technology publications define specific security controls for critical functions including Smart Grid, overall Cybersecurity Framework, Cloud Computing, Computer Security Resource Center, Information Technology Laboratory, National Cybersecurity Center of Excellence (NCCoE). For this reason, the NIST requirements are typically utilized by large enterprises to augment the structure introduced by compliance with the ISO/IEC 27000 Series.

6. *Security Framework for Cloud Providers*

- i. *Identify the key elements and value of standardized security requirements for cloud-based solution providers.*

Standards are critical to ensure cost-effective and achievable migration, to ensure that mission-critical requirements can be met, and to reduce the risk that sizable investments may become prematurely technologically obsolete. Standards are key elements required to ensure that Exelon data, services, and solution components are managed, secured and hardened in accordance with the sensitivity of the underlying data and the criticality of the service or solution.

- ii. *Identify and explain the security best-practices framework you would recommend the Commission adopt for cloud services. Explain how this framework differs from security best-practices you would recommend for on-premise systems.*

ComEd recommends the ISO/IEC 27000 / 27018 as the overall Information Security framework, with implementation of the necessary corresponding Security Controls as defined by NIST. The NIST Risk Management Framework (DIACAP) with SCAP validation should also be implemented where required.

The ISO/IEC 27000 series of published information technology and information security documents provide scope, normative references, and security control objectives to act as a model and set of guidelines to define a framework of information security policies and security control objectives for enterprises requiring a structured, holistic, and systemic approach to information security;

The ISO/IEC 27018:2014: "*Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*" establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. In particular, ISO/IEC 27018:2014 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services. The ISO/IEC 27000 series defines Security Control Objectives (e.g., "encrypt data"), but does not define the exact security control required (e.g., "encrypt data utilizing AES 256 XTS Mode"); and

The current NIST Information Technology publications define specific security controls for critical Exelon functions including Smart Grid and provide an overall Cybersecurity Framework for Cloud Computing. For this reason, the NIST requirements should be utilized to augment and supplement the structure introduced by compliance with the ISO/IEC 27000 series. NIST defines proper security controls required to secure the underlying data, services, and solutions.

- iii. Identify the key elements and value of standardized due diligence guidelines for utilities when selecting cloud-based solution providers. Explain how this guidance is different from selecting on-premise solutions.*

Utilities should review several key elements when performing due diligence with regard to cloud providers. Providers should incorporate industry-compliant measures focused on ensuring the security and confidentiality of all critical business, including all customer data that is either stored, processed, or transmitted through the cloud-based systems and infrastructures. Some key elements include the processes the providers use in managing security audit evidence, including requiring the provider's to execute due diligence preparation and review of audit reports such as Statements on Standards for Attestation Engagements (SSAE) 16 reports. In addition, cloud providers should evidence their alignment with ISO/IEC

27001 certification, which certifies compliance with information security controls published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Other certifications to review when conducting due diligence evaluations of cloud-solution providers include PCI DSS, HIPAA, and FIPS 140-2. While not as broad as SSAE 16 and ISO 27001, these additional governance frameworks nevertheless demonstrate a provider's high level of commitment to security;

Finally, utilities should consider the kind of data encryption applied by solution providers with a given implemented and deployed hosted model. Encryption means that the contents of files and documents are scrambled and encoded using a computer algorithm. Users who have permission to view the files can decode them, but anyone else who attempts to view the files would see only incomprehensible information. The Advanced Encryption Standard with a level of 256 bits (AES-256) is an example of one widely used standard to protect sensitive information. AES-256 is relevant to data, both in transit and at rest, and is used by utility operations, financial institutions, banks, and e-commerce Web sites.

Utilities should incorporate these standards similarly into their on-premise solutions.

- iv. *Identify the cloud services selection guidelines you would recommend for Commission adoption and explain why.*

Exelon has established a Cloud computing Security Requirements Matrix, which describes Exelon's architectural security controls required for data stored with a Cloud provider. In addition a Vendor Security Questionnaire has been created which describes Exelon's security policies, guidelines, and procedures for Cloud Solution providers. These two documents together are applicable to all of the operating companies under Exelon and constitute Exelon's security requirements for Cloud providers providing a robust evaluation of data encryption, access control, data sensitivity classification, and multi factor authentication.

7. *Best Practices*

- i. *Describe how best practices in protecting sensitive utility and customer information differ between cloud-based hosting and on-premise hosting.*

When storing data with a Cloud Service provider or when utilizing a Cloud-hosted solution, it is incumbent upon the utility to ensure the appropriate same or greater security controls are in place as would be

if the solution or data were hosted in an on-premise data center. Even with the most stringent 3rd party requirements and controls, there is some loss of control of the data or solution, simply because it is outside of the utility's direct control. The CloudSRM (Security Requirements Matrix) and VSQ (Vendor Security Questionnaire) are designed to ensure that sufficiently stringent compensating security controls are in place to maintain a specific utility's control of the data, service, or solution.

8. Compliance

- i. *Describe whether and how cloud based solutions can improve utility compliance, privacy, and data security.*

Utilizing a vendor who has achieved a Compliance or Regulatory Certification to store or process utility data can result in significant cost savings as compared to an internal regulatory certification initiative. Privacy, data security, and access control can be centralized in a Cloud solution, regardless of who is accessing the data or from where; for data Classified as Confidential or Restricted Confidential, Cloud-service providers are required to encrypt all data in transit and in storage, which is a more stringent requirement than data in storage in a typical on-premise solution.

9. What Should Utilities Avoid Putting in the Cloud?

- i. *Describe the utility functions - including generation, transmission, distribution, metering, consumption, customer data management and customer experience - that should not be placed in the cloud and explain why. Would your answer depend on whether the information was placed in a public versus private cloud?*

Utilities should generally avoid putting data classified as NERC or SCADA or classified as restricted confidential into the cloud. In addition, data directly related to internal security configurations (e.g., internal firewall rules, Remote Access / VPN configuration files, etc.) or data which could be used to deduce or infer internal, proprietary processes or activities (e.g. use of tools utilized to repair a steam leak in a plant, or purchase orders for replacement parts ordered due to sabotage or eco-terrorism, etc.) should also not be stored in the cloud.

With regard to meter or customer data, data classified as PII should not be stored in a Public Cloud, as opposed to a Private Cloud. Depending upon the sensitivity of the data being stored with the Cloud provider, Exelon may request a Private Cloud solution. Exelon's current relationships with Oracle Cloud and Microsoft Azure would allow Exelon to move data

into a "Private Cloud"-type solution if dictated by the business requirements or the results of a comprehensive Risk Assessment.

10. *Connectivity*

- i. *Describe how existing utility IT systems that are not currently interconnected can be made to integrate if hosted in the cloud. What are the benefits and vulnerabilities introduced by interconnecting various utility IT services?*

Existing IT systems which perform the same or similar function, but have evolved as siloed, utility-specific solutions, could consolidate into a single solution via Cloud technology. The benefits of such a solution include greater availability and reduced operational and support costs. Risks with this type of solution are similar to any Cloud solution: Loss of direct control over the data or solution by the utility, reliance on internet connectivity and DNS (Domain Name Service) and ensuring data is encrypted at the appropriate level whether in transit or in storage.

Regulatory Barriers:

A. **Ratemaking Treatment:**

1. *Does current ratemaking practice discourage Illinois utilities from deploying cloud-based solutions (e.g., data analytics) provided by third party vendors?*

As discussed in the response to Question 1 above, generally companies choose information technology solutions primarily based on operational factors, with cost as a secondary consideration. Regulatory treatment is also considered in order to develop a balanced scorecard on options to determine the best solution. Recent accounting guidance clarification coupled with current ratemaking practice may result in adverse financial consequences when choosing a Cloud solution. On April 15, 2015, the Financial Accounting Standards Board (FASB) issued Accounting Standards Update 2015-05, Customer's Accounting for Fees Paid in a Cloud Computing Arrangement. Attachment 1 to this response includes a PwC write-up on this guidance. Pursuant to this update, the FASB has clarified rules related to cloud computing, essentially defining costs that are currently capitalizable under on-premise solutions as expense if using cloud based solutions, unless specific criteria can be met. In summary, the rule requires a two part test in order to capitalize implementation costs paid to vendors for Cloud solutions not owned by the utility. Implementation costs can be capitalized if (1) the customer has the contractual right to take possession of the software at any time during the hosting period without significant penalty, AND (2) it is feasible for the

customer to either run the software on its own hardware or contract with another party unrelated to the vendor to host the software.

With an on-premise solution, generally installation costs are capitalizable allowing utilities to earn a return on the investment in IT systems. With a cloud based solution, if utilities do not meet the criteria to capitalize these costs, they will be treated as expense, and the utilities will lose the ability to earn a return on the investment.

2. *Describe any reasonable justification for accounting ratemaking distinction between investing in cloud-based solutions and investing in on-premise solutions.*

The ability for utilities to recover the costs of and earn a return on investments made in the provision of utility service is essential in supporting investment in Illinois' infrastructure. To maintain incentive to invest in IT solutions, ratemaking should not look different because a solution is on-premise versus cloud based.

3. *Describe whether and how utilities are adopting cloud-based solutions despite its accounting treatment.*

ComEd continues to explore cloud based solutions weighing the key considerations already discussed above; however, the current ratemaking treatment is a concern.

4. *Identify alternative ratemaking treatments that would render Illinois utilities indifferent in either choosing to deploy cloud-based solutions provided by third party vendors or continuing with on-premise IT systems owned by the utility.*

- 1) If a cloud based solution is treated as expense, allowing utilities to record the implementation costs related to that solution to FERC Account 303000 – General Intangible Plant would allow utilities to be indifferent with regard to ratemaking. The cost of the solution would be depreciated over its expected useful life. FERC Account 303000 is included in rate base, thus utilities would be allowed to earn a return on these investments just as with any other asset included in rate base.

- 2) As an alternative to #1, allowing utilities to record the costs related to cloud based solutions in a regulatory asset, amortized over the useful life of the solution would also be a way to include in rate base, earning a return just as any other asset included in rate base.

- i. *For each alternative identified, identify the costs and benefits of implementing that alternative.*

- 1) There is no additional cost related to alternative (1). The benefit with this ratemaking treatment would render Illinois utilities indifferent in choosing cloud based versus on-premise solutions.
- 2) There is no additional cost related to alternative (2). The benefit with this ratemaking treatment would render Illinois utilities indifferent in choosing cloud based versus on-premise solutions.

ii. *For each alternative identified, identify Illinois administrative rules that would need to be revised, and the revisions(s) required, in order to implement that alternative.*

N/A

B. Other Barriers:

1. *Identify and explain any other regulatory barriers that discourage Illinois utilities from deploying cloud-based solutions (e.g., data analytics) that would otherwise be in the best interest of the utility and its customers. For each barrier identified, identify Illinois administrative rules that would need to be revised, and the revision(s) required, to eliminate that barrier.*

N/A

Additional Benefits of Cloud Deployment:

1. *Describe the types of cloud-based technologies are available for electric, gas, and water utilities.*
2. *In electric utilities:*
 - i. *Identify specific software services not currently deployed in Illinois available to engage customers in distributed generation, distributed storage, demand response, and energy efficiency programs. Are those tools available as on-premise and cloud solutions, or is only one option available?*

In jurisdictions where there has been high penetration of DER (in the U.S. – Arizona, California, and Hawaii – and globally in Australia and Germany), utilities are deploying an overall Grid Management System that interacts with the electrical grid, encompassing all of the activities necessary to modernize the grid, including DER management, distribution grid operations, and planning functions. It provides advanced communications and the intelligence necessary to manage the electrical grid as a fully integrated network, which allows the injection and delivery of energy at any point, rather than treating it as a

unidirectional distribution system. Such an integrated model allows the optimal use of available resources to meet both reliability and cost priorities in a coordinated fashion.

The overall Grid Management System will be comprised of both enhanced functionality of existing software services (Distribution Management System, System Planning Tools) as well as new software services such as (1) DER and device control system that provides connectivity across all other systems and services and; (2) an economic system that interacts with markets and contracts to ensure that the economic implications of the distribution network are appropriately realized.

To date, these evolving software services have generally been made available as on-premise systems. Some data repository systems are now managed through cloud services, serving as the historian and librarian of the GMS, providing users and external systems access to time series data and salient records of its performance and activities.

- ii. *Identify specific services not currently deployed in Illinois that could provide customer engagement portals that improve customer engagement; increase customer satisfaction; and help meet regulatory mandates for verified energy savings and demand reduction.*

There are specific services that are not currently available from all customer engagement portals. It is difficult to determine the deployment level in Illinois because most are offered as behind-the-meter solutions that usually do not require utility involvement. The following are specific services that can be used to verify energy savings and demand reduction and increase customer engagement and satisfaction:

- **Conservation analytics** – Potential for utilities to more effectively target buildings for energy savings, engage customers with customized opportunities, and track savings at scale. Through the High-Performance Buildings Pilot Project in downtown Seattle, real-time data analysis of buildings is aimed at reducing power consumption.
- **Operational analytics** – The combination of granular visibility into systems and devices, coupled with big-picture analytics and insights, enables companies to increase operational efficiencies and reduce costs.

- **Demand Analysis** – The purpose of demand analysis is to provide detailed information about how a facility, building, service entrance, or any user of electricity uses energy. It is used for better assessing more efficient energy use.
- **Built-in Customer Service Analytics & Dashboards** – An example of a customer service dashboard is one offered by Oracle that measures call and electronic-message volumes by region, day of the week, hour of the day, and type of customer making the contact. This would be helpful for call center resource planning.
- **Provide EV charging information and locations, rates, and charging options** – Third party vendors such as EVConnect have created EV charging management and application platforms that have the capability of locating EV charging stations, monitoring the status of stations, setting charging pricing and tariffs for usage, notifications to charge station users, remote updating of firmware, reserve EV charging stations, and the ability to create management reports.
- **Smart Home Automation** – Smart Thermostats such as those offered by Nest and other vendors provide energy savings through efficient use of energy.
- **Peak Load Management** – Some demand response programs allow consumers to use direct load control programs to give the utility direct charge of the devices that control the loads during events where peak load is at its highest.

3. *In water and gas utilities:*

- i. *Identify the types of software or services not currently deployed in Illinois that could improve customer engagement and increase customer satisfaction.*

N/A

- ii. *Identify the types of software or services not currently deployed in Illinois that could detect leaks and inefficiencies, improve conservation, and lower operating costs.*

N/A

4. *Describe any additional feature benefits to a utility when adopting a cloud-based solution. For example, what are the benefits of cloud software that analyzes consumption patterns, identifies malfunctioning meters, reduces unbilled energy, or engages in predictive maintenance and load forecasting, among other things.*

Offering solutions via the Cloud allows utilities more options to find efficient and cost effective solutions that benefit the grid and utility customers. As noted throughout this response, utilities evaluate each situation on balance to determine the best solution. As more cloud offerings become available, utilities will have more optionality to best meet changing operational and customer needs.

Dated: April 29, 2016

Respectfully submitted,
COMMONWEALTH EDISON COMPANY

In depth

A look at current financial reporting issues



No. 2015-09
May 1, 2015

What's inside:

Background	1
Key provisions	1
Elimination of analogy to lease guidance	2
Financial statement implications	3
Transition and disclosure requirements	3
What's next	4

Cloud computing fees

FASB issues guidance on customer accounting

At a glance

On April 15, the FASB (the “Board”) issued new guidance on a customer’s accounting for fees paid in a cloud computing arrangement (CCA). Previously, there was no specific U.S. GAAP guidance on accounting for such fees from the customer’s perspective. Under the new standard, customers will apply the same criteria as vendors to determine whether a CCA contains a software license or is solely a service contract. For public companies, the new standard is effective for annual periods, including interim periods, beginning after December 15, 2015. For non-public companies, it is effective for annual periods beginning after December 15, 2015, and interim periods in annual periods beginning after December 15, 2016. Early adoption is permitted.

Background

.1 The lack of specific U.S. GAAP guidance on customer fees paid in a CCA has resulted in diversity in practice as to whether such fees are recorded as a software license or a service contract. The Board issued [Accounting Standards Update 2015-05, Customer’s Accounting for Fees Paid in a Cloud Computing Arrangement](#), as part of its simplification initiative to reduce the diversity in practice, and reduce the costs and complexity of assessing fees paid in a CCA. While the new standard does not provide explicit guidance on how to account for fees paid in a CCA, it does provide guidance on which existing accounting model should be applied.

.2 For purposes of applying the new guidance, a CCA includes software-as-a-service (SaaS) and SaaS-type services. “Hosting” refers to situations in which the end user does not take possession of the software; instead, the software resides on the vendor’s or a third party’s hardware, and the customer accesses the software remotely.

Key provisions

.3 Under the new standard, fees paid by a customer in a CCA will be within the scope of the internal-use software guidance if both of the following criteria are met:

- The customer has the contractual right to take possession of the software at any time during the CCA period without significant penalty.
- It is feasible for the customer to run the software on its own hardware (or to contract with another party to host the software).

.4 The standard provides some guidance on how to interpret the term “significant penalty.” The ability to take delivery of the underlying software without significant cost and to use that software separately without a significant reduction in value would indicate there is not a significant penalty. Determining whether taking possession of the software will result in significant penalty will require judgment.

.5 Arrangements that do not meet both of the criteria are considered service contracts, and separate accounting for a license will not be permitted. Arrangements that meet the criteria are considered multiple-element arrangements to purchase both a software license and a service of hosting the software. Existing guidance on internal-use software is applied to the purchased license.

.6 Costs incurred by a customer in a CCA that includes a software license should be allocated between the license and hosting elements. The consideration should be allocated based on the relative fair value of each element. Determining the fair value of the software license and hosting service may require the use of estimates. Management should consider all relevant information, such as information from the negotiation process with the vendor, in estimating the fair value of the license. More observable inputs might be available to estimate the fair value of the hosting element.

Elimination of analogy to lease guidance

.7 The new standard also eliminates the requirement that customers licensing internal-use software apply the leasing guidance by analogy to determine whether to record a software asset. Removing the analogy to the leasing guidance requires companies that purchase or license software to follow the same guidance for capitalization as any other purchased or licensed intangible asset.

.8 Currently, the internal-use software guidance requires companies to apply the leasing guidance by analogy because the software guidance was modeled after fixed asset accounting. If an entity uses a fixed asset without owning the asset, lease accounting would apply. Since a license is the use of another entity’s asset, to be consistent with the fixed asset model, current guidance requires a company to apply the leasing guidance by analogy in determining whether to record an asset.

.9 The Board decided, as part of the new standard, to make the accounting for acquired intangible assets consistent and eliminated the specific rule for internal-use software.

PwC observation:

The Board’s objective was to make the accounting for software licenses consistent with the accounting for all other licenses of intangible assets. The Board noted in the basis for conclusions to the new standard that this guidance could change the current accounting for those companies that treat a software license as an executory contract (that is, companies that do not record an asset by analogy to an operating lease). Therefore, the elimination of the analogy to lease accounting could cause more software assets to be capitalized. The recognition of an acquired intangible asset is required whether the intangible is acquired individually or as part of a group of assets.

Companies that determine they should record an asset for a software license may encounter operational difficulties in determining the amount and timing of capitalization for certain types of licenses, such as time-based licenses with auto renewal options.

If acquired as part of a group of assets, a software license will be capitalized at its relative fair value. Given the significant variability of the pricing of software, judgment will be required to determine the fair value of the software acquired for purposes of allocating the amount paid to all the acquired assets.

Financial statement implications

.10 A customer’s assessment of whether a CCA contains a software license could have a significant impact on its financial statements. For example, the accounting for an upfront fee paid in a CCA would differ depending on whether the fees are considered a payment for a software license or a prepayment for a service contract:

Financial statement	Internal-use software	Service contract
Balance sheet	Fixed or intangible asset	Prepaid asset
Income statement	Depreciation/amortization	Operating expense
Statement of cash flows	Investing activities	Operating activities

.11 Companies that expect to have a change in classification under the new standard should also assess the follow-on impact to other areas of the business, such as debt covenants and incentive compensation plans.

Transition and disclosure requirements

.12 Companies will have the option of transitioning to the new guidance either retrospectively, or prospectively for all new transactions entered into or materially modified after the date of adoption.

.13 Public companies adopting prospectively will disclose the following in the first interim period and annual period after the effective date:

- Nature of and reason for the change in accounting principle
- Method of transition
- A qualitative description of the financial statement line items affected by the change in the first interim and annual periods after the effective date

Attachment 1 to the Initial Comments of Commonwealth Edison Company

.14 Public companies adopting retrospectively will disclose the following in the first annual period, and the interim periods within that annual period, after the effective date:

- Nature of and reason for the change in accounting principle
- Method of transition
- Description of previously reported information that has been adjusted
- Effect of the change on income from continuing operations, net income, other impacted financial statement line items, and any impacted per-share results for the current and prior periods
- Cumulative effect of the change on retained earnings as of the beginning of the earliest period presented

.15 All other companies should make the disclosures for prospective transition or retrospective transition, as applicable, in the first annual period after the adoption date. If the company elects to early adopt in an interim period, the entity should also make those disclosures in the interim periods within the first annual period after the adoption date.

What's next

.16 The new standard is effective for public companies for annual periods, including interim periods within those annual periods, beginning after December 15, 2015. For non-public companies, it is effective for annual periods beginning after December 15, 2015, and interim periods in annual periods beginning after December 15, 2016. Early adoption is permitted for all companies.

.17 Prior to adoption, public companies should consider the disclosure requirements for recent accounting pronouncements detailed in Staff Accounting Bulletin (SAB) Topic 11-M (formerly SAB 74).

Questions?

PwC clients who have questions about this *In depth* should contact their engagement partner. Engagement teams who have questions should contact the Revenue team in the National Professional Services Group (1-973-236-7804).

Authored by:

Michael Coleman
Partner
Phone: 1-973-236-7237
Email: michael.coleman@us.pwc.com

Michael Sandusky
Senior Manager
Phone: 1-267-330-5199
Email: michael.r.sandusky@us.pwc.com

Jim French
Partner
Phone: 1-408-817-3968
Email: jim.french@us.pwc.com

Christopher Williams
Senior Manager
Phone: 1-973-236-5131
Email: christopher.r.williams@us.pwc.com