INL/RPT-24-78249
Revision 0

Use Case-Informed Framework for Utility Cloud Migration

White Paper

JANUARY 2024

Emma Stewart,
Julia Morgan, and
Remy Stolworthy

Idaho National Laboratory

CIRRUS
A cloud feasibility assessment tool

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

INL/RPT-24-78249

Use Case-Informed Framework for Utility Cloud Migration

White Paper

Emma Stewart,
Julia Morgan, and
Remy Stolworthy
Idaho National Laboratory

January 2024

Idaho National Laboratory
U.S. Department of Energy
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Infrastructure
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

EXECUTIVE SUMMARY

This white paper presents a comprehensive methodology for assessing utilities' cloud postures and frameworks. It aims to produce a roadmap and strategy for a cloud-enabled grid future, providing guidance for integrators, asset owners, and operators. Instead of offering a yes or no answer for cloud implementation, this framework offers strategic guidance on responsibly preparing for and deploying cloud solutions.

This paper delves into cloud-service models pertinent to the electric sector, dissecting the shared responsibility model and elucidating what on-premise infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) entail. A pivotal consideration within the context of the shared responsibility model is the allocation of responsibility for foundational security aspects—a decision that will be informed by a comprehensive risk assessment. The ensuing discussion will present a checklist of certifications necessary for a secure cloud transition, equipping utilities with the knowledge to navigate this digital transformation with confidence and with a strategic roadmap.

Furthermore, the paper outlines gaps in understanding the U.S. government's role in shaping technology development and responsible use. Its purpose is to aid decision-making by offering support for risk-informed solutions that benefit those managing assets and operating in the cloud environment. The primary objective is to enhance the resilience and future readiness of a decarbonized electric grid, with cloud solutions as one viable option. The paper synthesizes information on current and future grid architectures and applications, considering both conservative and progressive energy transitions, along with scalable and distributed computing considerations.

CONTENTS

FIGURES

TABLES

ACRONYMS

ADMS	Advanced Distribution Management System
AI	Artificial Intelligence
CIE	Cyber-Informed Engineering
CoT	Cloud of Things
CSP	Cloud Service Provider
DER	Distributed Energy Resources
DERMS	Distributed Energy Resource Management System
EC	Engineering Controls
EV	Electric Vehicles
GIS	Geographic Information System
HCE	High-Consequence Events
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicators
NERC	North American Electric Reliability Corporation
OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition

Use Case-Informed Framework for Utility Cloud Migration

1. INTRODUCTION

The advent of cloud computing has catalyzed a transformative shift across various industries, with the energy sector at the forefront of this revolution to standardize cloud migration. This white paper aims to identify use cases that will inform the development of a practical framework to guide utility companies in implementing cloud computing and present the framework.

Utilities, traditionally reliant on robust in-house information technology (IT) and operational technology (OT) infrastructures, are pivoting towards cloud implementation and digitized services for enhanced data management, email communications, and business operations. Some utilities are additionally considering operational and hybrid control functionality transitions to the cloud. In contrast, smaller utilities, often with less robust IT and OT infrastructures, rely on cloud technology to speed up their existing modernization efforts. These moves include leveraging access to high-powered computing resources and, perhaps more importantly, off-the-shelf software as a service (SaaS) solutions for managing and optimizing data, resulting in improved decision-making.

The impetus behind the push for a universal energy sector cloud migration is multifaceted. The evolution and diversity of energy sector resources necessitate adept and potentially computationally intensive distributed systems management, while digitalization ubiquity and microprocessor-based device use compel cloud-based solution implementation. These interconnected devices frequently automatically transmit data online for vendor processing and analysis. In some scenarios, access through a vendor portal is the only means of viewing specific data. Vendors may void warranty agreements in health monitoring cases if cloud computing is prohibited. Cloud services serve as a model of technological resilience with high redundancy and geographic dispersion, essential characteristics when combatting energy-related challenges like those experienced in Texas, California, Ukraine, and similar regions prone to natural disasters.

Furthermore, the utility sector leverages advanced analytics and artificial intelligence in decision-making, often integrating new operational products like advanced distribution management systems (ADMSs). This integration enhances operational efficiency and accelerates cloud-computing adoption across other government sectors. The connection between analytics, artificial intelligence (AI), and cloud computing is fundamental: cloud platforms provide the scalable infrastructure and computational power needed to process large datasets and run complex AI algorithms. This capability facilitates the deployment of AI-driven analytics tools. At the same time, a progressive mindset toward innovation increasingly reveals the limitations of in-house solutions, which often lag behind more forward-thinking cloud-based approaches.

Cloud computing in the energy sector presents a compelling economic proposition, enabling utilities to manage costs more effectively and concentrate on core business activities. Traditionally, organizations maintained their own servers in-house, requiring significant investments in hardware, software, and skilled IT and OT personnel for ongoing management, maintenance, and security. With cloud computing, these capital expenditures are potentially reduced, as companies no longer need to purchase and maintain physical servers. Instead, they pay for cloud services on a subscription basis, offloading server management to cloud providers who ensure secure network management and updates. However, cloud adoption is not without its own challenges, particularly related to security and the shared responsibility it creates. In some cases, associated human capital costs can escalate to untenable levels if not monitored. Additionally, costs related to data transfer, compliance, integration, and ongoing cloud service fees can accumulate over time, potentially offsetting some of the initial savings. Cloud computing also establishes an additional risk area if stakeholder access control, data protection measures, and consequence-focused engineering controls (ECs) are not properly established or implemented. Therefore, because of these considerations, utilities require a scalable cloud computing security framework that is cost-effective and operationally efficient and enables responsible consequence-driven approaches.

As seen in Figure 1, cloud technology integration into the energy distribution system disrupts the traditional flow of information. The information flow in a traditional system moves directly from the large-scale electricity producer to the utility company. The utility company maintains responsibility for defining electricity distribution quantities and costs associated with end-user consumption. However, when utilities leverage cloud services such as generation, distribution, and consumption, data is sent to the cloud instead of the utility. Though it is possible that the utility would own the cloud infrastructure, there is also a chance that the cloud technology is contracted to a third-party administrator. Considering this scenario, Figure 1 displays the cloud as a separate entity from the utility.

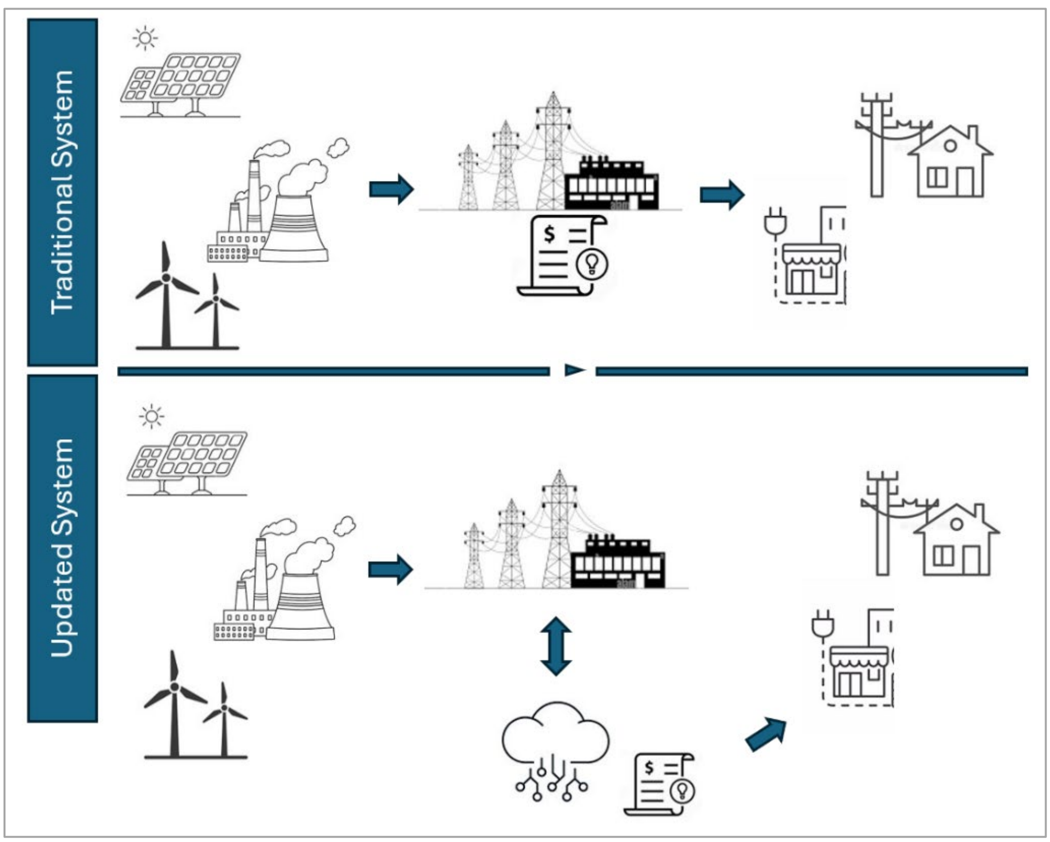

Figure 1. The information flow for an energy distribution system before and after cloud solutions are integrated.

Within the energy space, cloud migration is taking shape in diverse forms, with utilities taking the following proactive steps:

1. Utilizing cloud services to improve IT and OT capabilities, optimizing operations such as data management, email, and various business processes.
2. Implementing cloud solutions alongside existing OT systems can significantly boost operational efficiency. Cloud computing integrates real-time data across IT and OT systems, enabling better decision-making and faster issue resolution.
3. Adopting cloud solutions to modernize and adapt to new digital applications, such as distributed energy resource management systems (DERMS), enhances operational efficiency by providing scalable and flexible resources. This allows organizations to deploy, manage, and update applications more quickly, streamline workflows, and respond to changing business needs without traditional infrastructure constraints.
4. Embracing third-party integrators facilitating cloud adoption by providing system-wide cloud services for highly dispersed fleet orchestration and management.
5. Understanding that software vendors are offering specialized cloud platforms designed to meet the unique needs of the energy sector.
6. Acknowledging that hardware vendors are finding efficiencies through cloud-based data collection and fleet asset management, offering new revenue streams through enhanced service agreements.

Cloud demand is rising primarily due to cloud services' scalability and flexibility. Businesses can easily scale their computing resources up or down based on demand, which is far more cost-effective than investing in traditional on-premises infrastructure. This adaptability enables organizations to quickly respond to changing market conditions, launch new products, or expand into new markets without the need for significant upfront investments in hardware. Additionally, the growing need for remote work solutions, digital transformation, and increased data storage and processing capabilities further fuels the demand for cloud services.[1] These factors combined make cloud computing an attractive option for businesses across various industries.

As energy delivery infrastructure expands to meet consumer demand, cloud computing integrated with the Internet of Things (IoT) provides a scalable, efficient platform for DERMS. The Cloud of Things (CoT) creates a network of systems architecture with increased resilience and improved connectivity. The CoT significantly enhances efficiency and scalability by integrating the IoTs with cloud computing. This integration addresses the challenges posed by the massive number of IoT-enabled devices and the vast volumes of data they generate. Storing and processing this data locally becomes impractical, necessitating the use of cloud resources. CoT allows for remote monitoring, management, and control of IoT devices, making it easier to manage large-scale deployments.

By leveraging cloud-based resources, CoT offers virtualized storage and computing power, which can be scaled dynamically to meet demand. This scalability ensures that businesses can efficiently process and analyze data, leading to more advanced smart applications across various domains. The various service models within CoT, such as Sensing-as-a-Service and Big-Data-Analytics-as-a-Service, further enhance its capability to support diverse IoT applications, thus improving overall efficiency and scalability in connected environments.[2]

[1] Forbes Tech Council. *Powering the Growth of Cloud Computing: Infrastructure Challenges and Solutions*. July 24, 2023. https://www.forbes.com/councils/forbestechcouncil/2023/07/24/powering-the-growth-of-cloud-computing-infrastructure-challenges-and-solutions/.

[2] GeeksforGeeks. *Introduction of Cloud of Things (CoT)*. Accessed August 9, 2024. https://www.geeksforgeeks.org/introduction-of-cloud-of-things-cot/.

Additionally, as OT operationalizes cloud-based cybersecurity systems, it effectively becomes the most secure zone in an energy distribution network through segmentation, as explained by the Purdue Model for industrial control systems (ICS).[3] Policy, application, and need necessitate some interconnectedness within the ICS. Industrial Control Systems as a Service is a new breed of controls in the cloud also being considered, primarily for distributed energy resources (DER) Management and new digital products. While some interconnectedness within ICS is necessary to meet policy, application, and regulatory requirements, it must still comply with all relevant industry, state, and federal standards.

The U.S. government identifies sixteen types of infrastructure as critical because of their importance in providing the fundamental necessities of modern society.[4] While all sectors are considering cloud migration in some form, the energy, communications, water, and transportation infrastructure overseeing bodies are primarily considering cloud architectures for service delivery. These sectors are operated autonomously yet are entirely interconnected. Their interconnectivity creates a complex system in which cloud-based applications can be both beneficial and detrimental to their primary delivery function. Cyber-physical systems provide the mechanism for the interconnection of cloud and other infrastructures.[5]

As the demands on critical infrastructure increase, large-scale critical infrastructure systems distributors require a robust methodology for sustaining functionality in the event of a digital or physical catastrophic event. According to ABI Research, cybersecurity investments are estimated to increase by 83% by 2027 to maintain a resilient critical infrastructure system.[6] Integrating cloud technology into critical infrastructure sectors improves the underlying cybersecurity protections by creating a platform to increase overall data storage, computation, and visualization capabilities.[7]

2. ELECTRIC GRID CLOUD USE CASES

Cloud technology implementation within utility infrastructures is not only a current trend but a pivotal element in driving equitable modernization across various scales of energy operations. The use cases highlighted herein detail innovative approaches and the convergence of cloud computing with the operational and practical needs of utilities. Following these use case descriptions, a framework is proposed to highlight these benefits and encourage additional utility adoption.

---

[3] Garton. Daniel. "Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation." National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure, November 12, 2019. https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf.

[4] Department of Homeland Security. "Critical Infrastructure." Accessed August 9, 2024. https://www.dhs.gov/science-and-technology/critical-infrastructure.

[5] Rinaldi, Steven M., Peerenboom, James P. and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, 21, no. 6, (December 2001): 11-25.

[6] ABI Research. "With COVID-19 Behind, New Cybersecurity Spend in Critical Infrastructure to Reach US$236 Billion by 2027," Last modified: May 16, 2023. Accessed August 9, 2024. https://www.abiresearch.com/press/with-covid-19-behind-new-cybersecurity-spend-in-critical-infrastructure-to-reach-us236-billion-by-2027/.

[7] Younis, Younis A., Merabti, Madjid, and Kashif Kifayat, "Secure Cloud Computing for Critical Infrastructure: A Survey," The 14th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking, and Broadcasting, (June 2013): 599-610.

2.1. Grid Management and Optimization

All sizes of utilities (small, medium, and large) are leveraging cloud solutions to manage the grid, optimize distribution, and incorporate data analytics for real-time operations. In turn, these utilities are yielding improved grid stability and enhanced customer engagement. The primary instances of cloud integration among small and medium utilities are ADMS-based grid management platforms. These cloud-based solutions provide real-time visibility into grid operations, enabling utilities to optimize power distribution, manage demand fluctuations, and prevent outages. Using cloud-powered analytics, utilities can also review vast amounts of data from sensors and smart meters to identify patterns, predict potential disruptions, and implement proactive energy measures. This cloud-based functionality improves utility reliability, drives savings, and helps to prevent potential safety issues. The underlying benefits of implementing cloud solutions for grid management and optimization include:

- Improved grid stability and reliability.
- Reduced energy losses and carbon emissions.
- Enhanced demand-side management and customer engagement.

Integrating cloud solutions, and specifically adopting a cloud-based ADMS platform, bolsters existing grid management and optimization efforts.

2.1.1. Advanced Distribution Management Systems

Adopting an Advanced Distribution Management System (ADMS) software platform represents a forward leap for utilities in more effectively managing their distribution networks. By leveraging the platform's cloud capabilities, ADMS software can better respond to pressing needs such as outage management, voltage optimization, and DERs management with greater efficiency and scalability. This allows for real-time decision-making and enhanced coordination during demand fluctuations and unforeseen outages, ultimately leading to a more reliable power distribution system. The cloud facilitates improved data processing and analytics, providing utilities with the critical insights needed to anticipate, diagnose, and respond to system anomalies swiftly. The benefits of using an ADMS platform in conjunction with cloud solutions include:

- Minimized outage and efficient restoration.
- Increased efficiency in energy distribution.
- Enhanced demand management.
- Greater ability to integrate strategic planning.

An ADMS platform can also integrate with asset management and predictive maintenance cloud-based software, creating a holistic approach to energy distribution.

2.1.2. Asset Management and Predictive Maintenance

Through predictive analytics and machine learning, cloud platforms facilitate comprehensive asset management, extending energy infrastructure lifespan and streamlining maintenance protocols. This asset management and maintenance is evident within utility companies like Électricité de France and National Grid. Cloud-based asset management systems can track the health and performance of critical energy infrastructure components, with the resulting data analyzed using machine learning algorithms to enhance predictive maintenance, improve operational efficiency, and reduce the risk of unexpected failures. The benefits of utilizing asset management and predictive maintenance via the cloud include:

- Extended asset lifespan and reduced maintenance costs.
- Improved operational efficiency and reduced outages.
- Enhanced safety and risk mitigation.

The benefits of cloud-based asset management and predictive maintenance are numerous. Data stored in the cloud can also be leveraged through data management and planning tools to improve efficiencies.

2.1.3. Data Management and Planning

An increase in distributed and digitized equipment deployment has exponentially expanded the type, frequency, and size of utility data collected. As standard communication methods have advanced to provide high-speed, high bandwidth channels for data transfer, the energy sector has found ways to leverage this data to inform real-time operations, proactive monitoring, and more informed decision-making surrounding planning processes. Cloud computing supports utility database access and management, along with options for increased storage and frequent backups. Access to near real-time information and developing computing algorithms to process the data is imperative to making strategic planning decisions. The benefits of these cloud-based data management and planning tools include:

- Better informed decision-making processes for short- and long-term planning.
- Enhanced data management and processing that data into usable information.
- Improved reliability and flexibility in structure for managing access to data from a variety of sources.

Smart metering and the associated data analytics go hand in hand with these cloud solutions.

2.1.4. Smart Metering and Enhanced Data Analytics

Real-time data from cloud-integrated smart meters enable personalized energy solutions and proactive demand-side management, fostering an environment for targeted consumer energy efficiency programs. Utilities have access to granular levels of monitoring and control that were previously impossible. Cloud-connected smart meters provide real-time energy-consumption data so consumers can make better-informed decisions. This allows utilities to offer personalized pricing plans, identify energy-saving opportunities, and detect anomalies in consumer usage patterns. From the utility side, dynamic demand response may be used for intelligent demand management and reduction of peak load. The benefits of smart meters and enhanced data analytics include:

- Empowered customers with personalized energy usage data.
- Improved customer satisfaction and loyalty.
- Data-driven decision-making for targeted energy efficiency programs.
- Improved outage service recovery with customer visibility.

While ADMS platforms utilize the cloud to focus on complete network monitoring, automated switching responses, outage management, and grid maintenance, DERMS leverage the cloud to concentrate on the wide variety of ways that DERs interact with the distribution network and are orchestrated for the energy market.

2.1.5. Distributed Energy Resource Management System

Cloud-based DERMS platforms enable seamless integration of renewable energy sources, improving grid resilience and reducing reliance on traditional energy generation methods. Most DERs do not interact directly with one another. A DERMS ensures that DERs are wholly utilized to supply grid support functions, maximize profit through energy arbitrage, and reduce peak loads and transmission congestion. DERs function in a coordinated fashion across multiple energy assets. DERMS are needed to aggregate data and make real-time decisions about energy dispatch and controls. Cloud-based DERMS platforms can aggregate, manage, and optimize DERs like solar panels, wind turbines, and energy storage systems (ESS). This technology enables utilities to integrate DERs seamlessly into the grid, balancing supply and demand and enhancing grid flexibility. The benefits of implementing a DERMS-based approach include:

- Greater flexibility of grid operations.
- Greater load and demand accuracy.
- Improved cost savings through intelligent energy dispatch.

In addition to improving grid management and optimization, cloud solutions can vastly heighten cybersecurity and compliance measures.

2.2. Cybersecurity and Compliance

Cloud platforms offer security tools that help meet energy compliance metrics, along with meeting industry standards and safeguarding sensitive information with the segregation of data networks. These solutions range from small, islanded grids to large-scale utility. The cybersecurity and compliance tools afforded by cloud solutions benefit historically under-resourced utilities that do not have the time, funding, or expertise to wade through necessary compliance processes themselves manually. The added benefit of integrated cloud software includes:

- Improved grid flexibility and resilience.
- Improve the level playing field among utility companies striving to enhance their cybersecurity efforts with cloud platforms.

2.2.1. Operational Continuity and Disaster Recovery

In line with single point of failure (SPOF), ensuring operational continuity is crucial for utilities relying on cloud-based systems. Disaster recovery plans and redundancies must be in place to mitigate risks associated with unforeseen events such as natural disasters, cyberattacks, or cloud service outages. This includes assessing the cloud provider's disaster recovery capabilities and whether the utility's specific needs align with disaster recovery plans and redundancies. For example, the New Hampshire Public Utilities Commission used three characteristics when performing their risk assessment associated with asset management: (1) changing technology, (2) regulatory, and (3) customer.[8] Using these three categories affords specific overlap with each risk-prone category, which can be addressed through cloud technology, as seen in Figure 2.

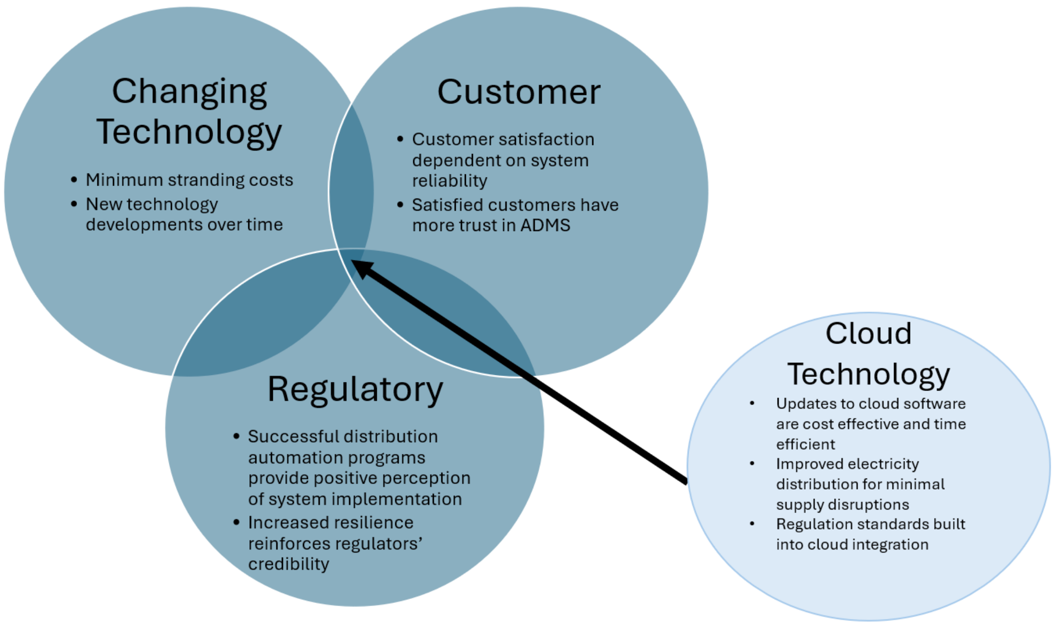

Figure 2. Representation of overlapping risks that are addressed by cloud technology.

A thorough risk assessment approach that encompasses data security, vendor considerations, regulatory compliance, network reliability, seamless integration, and robust contingency planning is imperative for utilities embracing cloud computing. By addressing these risks, utilities can include the benefits of cloud technology while safeguarding the integrity and resilience of their critical operations.

[8] Liberty-NH, Distribution Line Overarching Strategy, New Hampshire Public Utilities Commission, January 2019. Accessed August 11, 2024. https://www.puc.nh.gov/Regulatory/Docketbk/2019/19-120/TESTIMONY/19-120_2019-12-04_GSEC_ATT_REV_TESTIMONY_JOHNSON_RIVERA_STRABONE_TEBBETTS.PDF.

2.2.2. Equitable Technology Access and Cyber Resilience

The utility sector is at a crossroads, with a growing divide between large and small entities that can afford cutting-edge cybersecurity tools and the latest operational solutions. Many smaller entities are getting by with limited resources or band-aid solutions. Cloud services from top-tier providers offer a viable path to modernization, with managed security teams and outage prevention capabilities that serve both the most vulnerable and those able to invest in advanced solutions. Cloud-based cybersecurity solutions can protect against cybersecurity attacks, data breaches, and unauthorized access to sensitive information. Cloud providers offer advanced security measures, including encryption, firewalls, and intrusion-detection systems to safeguard utility data and comply with industry regulations. The benefits to utilities afforded by increased accessibility made possible by the integration of cloud solutions include:

- Enhanced cybersecurity posture and reduced risk of data breaches.
- Improved compliance with industry standards and regulatory requirements.
- Reduced digital infrastructure costs.
- Increased access to the latest tools for enhanced utility cybersecurity.

The correlation between access and improved cyber resilience for utilities is evident. Meanwhile, small utility companies see even greater benefits from cloud migration.

2.3. Small Utility Advantages

Small utilities see advantages of cloud computing that may differ slightly from their larger-scale counterparts because they are typically already attempting to do more with less. The increased ability to use off-the-shelf supervisory control and data acquisition (SCADA) is valuable for small utilities. Standalone SCADA and other similar products are cost-prohibitive for those utilities already on a shoestring budget. Additionally, these smaller utilities frequently need more staff to maintain and adjust to the changing cybersecurity landscape in these complex environments. Additional benefits to small utilities include:

- Improved access to Secure Emergency Management Systems.
- Enhanced customer satisfaction and outage management.
- Increased collaboration opportunities through equipment maintenance and asset management to share data between entities for improved analytics, effectively enlarging the data pool for more advanced functions typically ineffective in small silos.
- Strengthened reliability and planning models.
- Informed engineering drawing management.

Small utilities unequivocally witness several benefits of integrating cloud computing into their operations. The following summarizes the existing published use cases.

2.4. Company-specific Use Cases

Table 1 identifies the known cloud technology implementations existing today in the utility space. Each scenario is described by location, use case, and end-user scale. The location includes the city, state (if applicable), and country, which is valuable information for understanding technology accessibility globally. Scale is described as small, medium, or large, depending on the quantity of electricity distributed to end users. Additionally, each use case is identified by one of the previously established integration characteristics.

Table 1. Electric utility cloud integration use cases.

Company Name	Location	Scale	Use Case(s)
Enel[9]	Andover, Massachusetts, U.S.	Small (1.4 GWh)	Grid Management and Optimization, Data Analytics
Duke Energy[10]	Charlotte, North Carolina, U.S.	Small (1.7 GWh)	Grid Management and Optimization, Data Analytics
National Grid[11,12]	Waltham, Massachusetts, U.S.	Medium (2.4 GWh)	Asset Management, Grid Management and Optimization, Data Analytics
Vestas[13]	Boston, Massachusetts, U.S.	Medium (45 GWh)	DERMS, Security, and Compliance
Électricité de France[14]	La Defense, France	Medium (120+ GWh)	DERMS, Asset Management, Smart Metering, and Data Analytics
Orsted[15]	Fredericia, Denmark	Large (35.6 TWh)	Grid Management and Operations
E.On[16]	Essen, Germany	Large (261.7 TWh) (Statista, 2023)	Asset Management, Grid Management and Optimization, Data Analytics, Security, and Compliance

[9] Enel Group, "Enel 'Full Cloud': All the Advantages of Being the Pioneers." Last modified: July 11, 2019. Accessed August 9, 2024. https://www.enel.com/company/stories/articles/2019/07/enel-moves-cloud-model-future.

[10] Duke Energy Corporation, "Duke Energy Collaborates with AWS to Develop Smart Grid Solutions to Better Serve Customers and Drive its Clean Energy Transition." Last modified: November 17, 2022. Accessed August 9, 2024.

[11] National Grid, "Driving our Digital Transformation," Accessed August 11, 2024. https://www.nationalgrid.com/digital.

[12] Rooney, Paula. "National Grid's Energy Transformation is Fueled by IT," CIO, May 2022. Accessed August 11, 2024. https://www.cio.com/article/350316/national-grids-energy-transformation-is-fueled-by-it.html.

[13] Vestas, "Digital Services." Accessed August 11, 2024. https://www.vestas.com/en/energy-solutions/service/digital-services.

[14] Contino. "Accelerating Innovation and Cloud Adoption at EDF with a Cloud-Native Landing Zone and Operating Model in Just Ten Weeks." Accessed August 11, 2024. https://www.contino.io/case-studies/EDF-Cloud-Adoption.

[15] Orsted A/S. "Building More Than Ever Before." Accessed August 11, 2024. https://orsted.com/.

[16] E.On. "E.ON Ectocloud: Intelligent Control."Accessed August 11, 2024. https://www.eon.se/en_US/foeretag/ectogrid/ectocloud.

Cloud technology is a catalyst and a new risk class for an efficient, resilient, and digitized future grid. The outlined use cases serve as a testament to the cloud's potential to transform the utility sector's infrastructure, address the cybersecurity divide, and pave the way for sustainable energy pathways. Risk, consequences, and adequate protections must be considered to secure future success.

3. ADOPTION STAKEHOLDERS AND USERS

With every dip into the innovation pool comes a certain level of risk. Managing these risks is a top priority for critical infrastructure owners and operators, especially within the energy delivery sector. Utilities, in particular, bear the brunt of potential risks associated with cloud-related disruptions, as they are the primary users of cloud technologies within the energy sector. Given their significant exposure, it is crucial that utilities take careful steps when considering cloud migration. To this end, the following steps have been undertaken to inform the development of a proposed cloud migration framework and to outline key considerations that utilities must keep in mind as they navigate this complex landscape. Within the energy sector, utilities will be the primary cloud users; therefore, the following steps were taken to inform the proposed cloud migration framework and key considerations:

- Assess potential consequences by evaluating the impacts of cloud outages or vulnerabilities on electricity generation, transmission, and distribution.
- Prioritize risks and mitigation efforts by identifying critical systems and data most susceptible to cloud disruptions.
- Inform decision-making by guiding cloud adoption decisions, vendor selection, and risk management strategies.
- Assess operational failures and ability to dispatch resources accurately.
- Detect and notify vulnerability and threat information in real-time.

The proposed framework includes an energy delivery cloud risk assessment, focusing on the potential impact on utilities and third-party vendors while encompassing the perspectives of a diverse range of stakeholders and users. Understanding these primary and secondary stakeholder roles, responsibilities, and needs is imperative for designing a practical and comprehensive migration framework.

3.1. Primary Stakeholders

As more distributed resources and digital technology are added to the electrical grid, energy delivery ecosystems include a growing number of stakeholders. Each stakeholder may use cloud computing or cloud services for various aspects of their operational functions and to different degrees. The following section highlights many of the business functions that can benefit from cloud solutions, including the specific users of the technology and how they could interact with cloud infrastructure if integrated into their operations.

3.1.1. Utilities

Utilities might host their internal cloud applications or leverage services from external providers. Utilities are often subject to higher levels of regulation than other stakeholders in this ecosystem due to their ownership and responsibility for reliability to their customer base. This may limit the number and types of outside partnerships allowed. The following utility stakeholders should perform their own risk assessments; however, cloud risk mitigation steps for utilities can include more formal limitations or risk transfer to third-party administrators, as appropriate. The essential functions in which utilities can opt to use cloud services include:

- Demand management
- Predictive forecasting

- Strategic planning
- Service reliability
- Systems control
- Compliance management
- Cybersecurity threat prevention and control

Within the utility sector, additional primary stakeholders can also choose to adopt cloud technologies.

3.1.2. Maintenance Companies

Maintenance providers can have temporary or persistent access to power system data as part of their contracted service agreements. Maintainers may also have independent data streams collected in an independent cloud or be granted access to vendor or utility cloud services to view and manage data. Essential cloud functions for maintainers include:

- Asset health monitoring and proactive maintenance (reduced downtime).
- Improved planning for maintenance windows.
- Proactive response to potential threats.

These maintainers would greatly benefit from cloud solutions within their work.

3.1.3. Vendors

Vendors and aggregators of digital energy products are more commonly selling products that come standard with cloud-based applications. For example, battery energy storage systems often come with a standard cloud-based fleet monitoring solution. In many cases, product users such as utilities must create an account and log into the vendor's cloud-based portal to view and manage settings on the utility's equipment. This provides vendors with the opportunity to monetize service agreements. Cloud-based features, which vendors can provide, include:

- Asset health monitoring
- Improvements to future designs based on field data
- Software updates (features and security fixes)
- Optimization of resources
- Market participation
- Fleet management

Vendors can be an asset in cloud migration for utilities.

3.1.4. Regulatory Agencies

Governing bodies like the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) ensure grid security and reliability. They require utilities to assess and manage risks, making the value of cloud adoption in terms of regulation include:

- Compliance by demonstrating conformance to regulatory requirements for cybersecurity and risk management.
- Oversight involving monitoring utility risk assessments and intervening when necessary.

- Industry-wide analysis identifying systemic cloud-related risks across the energy sector.
- Streamlining reporting and auditing of assets and data deemed to be under NERC and FERC standards.

Cloud solutions can make utility operations more efficient, thus more easily meeting regulatory standards.

3.2. Secondary Stakeholders

Cloud service providers (CSP), cloud-based technology vendors, and cybersecurity firms play a crucial role in securing energy-delivery systems. These secondary stakeholders also benefit from the cloud migration in the following ways:

- Increased security by highlighting their cloud offerings' resilience to utilities and regulators.
- Improved services by identifying vulnerabilities in their own cloud infrastructure and services.
- Collaboration by engaging with utilities and regulators to develop best practices for secure cloud adoption.

Consumers can also be considered secondary stakeholders for the purposes of establishing the cloud migration framework.

3.2.1. Consumers

Consumers have a vested interest in a secure and reliable energy grid, making them a secondary stakeholder in cloud solution adoption. Ways in which cloud solutions within the utility sector indirectly benefit them include:

- Minimizes disruptions by reducing the likelihood and duration of power outages caused by cloud issues.
- Protects critical infrastructure by enhancing the security of energy delivery systems and safeguarding against cyberattacks.
- Enables energy efficiency management.

In relation to stakeholders, there are additional tangential groups that could be impacted by moving to the cloud.

3.3. Additional User Considerations

While not necessarily primary or secondary stakeholders, there are additional groups to consider when transitioning to cloud-based technologies, which include:

- Researchers and academics can utilize the transition as a valuable resource for research and analysis, informing future developments in cloud security and risk management for critical infrastructure.
- Public interest groups and organizations concerned with energy security and consumer protection can leverage the implications of cloud solutions to advocate for stronger safeguards in the energy sector.

This subset of additional users can also benefit from utilities leveraging the cloud.

4. CONSEQUENCES AND RISKS IN CLOUD DEPLOYMENT

While cloud computing offers significant advantages, it is equally important to acknowledge and address the potential risks and to consider the life cycle of the applications and their implications. The consequences and risks associated with cloud deployment help to paint a more holistic picture and contribute to a more practical migration framework.

4.1. Data Security, Privacy and Regulatory Compliance

Utilities should carefully evaluate cloud providers' security practices and ensure that their data is stored and managed according to industry standards and regulatory requirements. Initially, much of the responsibility for classifying and protecting the data lies with the utility, and methods for transfer should also be stringently considered. Data breaches and unauthorized access can have severe consequences for the utility, including financial loss, reputational damage, and customer trust erosion. Data stored in the cloud must also comply with NERC Critical Infrastructure Protection (CIP) standards and other regulatory compliance body stipulations. As previously mentioned, utilities operate in a highly regulated environment, and cloud adoption must adhere to not only specific data privacy guidelines but also cybersecurity and industry-specific standards. Careful due diligence and ongoing compliance monitoring are essential to avoid regulatory noncompliance and potential penalties. A cloud solution needs to have the ability to report and meet the metrics of each regulation or framework that is being implemented within the scope of the data stored or manipulated in the cloud.

4.2. Vendor Lock-In

Overreliance on a single cloud or technology provider can lead to vendor lock-in, making it difficult to switch providers or negotiate favorable terms later. After an initial assessment of benefits and consequences, utilities can adopt a multi-cloud strategy or hybrid cloud approach to mitigate this risk and maintain flexibility. Vendor lock-in should be evaluated from a cloud-provider perspective in terms of PaaS, IaaS, and SaaS, as well as the operational ability across energy-type sectors that will leverage cloud-native infrastructure.

4.3. Network Latency and Reliability

Cloud-based applications and services rely on reliable network connectivity. Utilities operating in remote areas with limited bandwidth may face latency issues that could impact critical grid operations. To provide equal access to new technologies associated with broadband networks, the Broadband, Equity, Access, and Deployment program assists in deploying and upgrading broadband access to traditionally marginalized or underrepresented areas.[17] Digital equity programs and cloud technology adoption programs assist in maintaining a community's complete participation in technology advancement and implementation. Locally stored and forwarded events in conjunction with cloud-based solutions ensure continuity in the event of network connectivity loss.

4.4. Legacy Systems Integration

Integrating cloud-based solutions with existing legacy systems can pose challenges, requiring careful planning, data migration strategies, and robust testing procedures. A seamless transition is crucial to avoid disruptions in operations and ensure the smooth functioning of critical systems. In addition to integration, it is imperative to maintain necessary information about the existing system. Often, change management will create a process to optimize legacy system integration. Two steps within this process that should be considered, especially for cloud-based solutions, are knowledge transfer and disruption reduction. These steps should be just two of an extensive process planned to fit the unique needs of the stakeholders.

---

[17] National Telecommunications and Information Administration, United States of American Department of Commerce, "Broadband Equity Access and Deployment Program," Accessed August 11, 2024. https://broadbandusa.ntia.doc.gov/funding-programs/broadband-equity-access-and-deployment-bead-program.

4.5. Single (or Uncontrolled) Point of Failure

If a utility relies on a third-party or vendor for data or control through their cloud system, there is a vulnerability wherein an attack or outage on the third-party could lead to significant consequences for the utility. This potential SPOF underscores the importance of contingency planning and risk mitigation strategies to safeguard against disruptions caused by uncontrollable external factors. Reasons for failure range from equipment deterioration to environmental disasters to a lack of server application availability. The effects of a SPOF can be mitigated by creating redundancies for critical components throughout the cloud architecture.[18]

4.6. Successful Cloud Deployment Case Studies

The following case studies highlight examples of successful cloud solution deployment and the positive impact on utilities around the world.

4.6.1. Ukrenergo, Ukraine

Ukrenergo, Ukraine's national power company, has encountered immense challenges during the ongoing conflict with Russia, particularly after the 2022 invasion. Missile strikes and cyberattacks have targeted its energy infrastructure, threatening the nation's power supply. To combat these threats and ensure resilience, Ukrenergo has relied heavily on Microsoft's cloud services. These services have been instrumental in maintaining operations, restoring damaged systems, and securing the grid.

With 8,000 employees working tirelessly to repair facilities, Ukrenergo leveraged Microsoft's cutting-edge technologies, such as Security Copilot, Sentinel, Azure, and Microsoft Defender for IoT. These tools provided real-time asset discovery, AI-driven threat analysis, and comprehensive security information and event management capabilities, which have been crucial for sustaining energy delivery. The integration of cloud solutions into critical infrastructure management has become increasingly vital in the face of political turmoil, enabling Ukrenergo to secure and reestablish the grid efficiently.

The deployment of these cloud technologies has not only ensured uninterrupted energy services but also exemplified the transformative potential of modern digital tools in safeguarding critical infrastructure during times of crisis. This approach underscores the indispensable role of cloud technology in enhancing the resilience and security of vital national systems amidst unprecedented challenges. Ukrenergo's experience stands as a testament to the power of innovation in overcoming adversity and maintaining stability in the energy sector.[19]

---

[18] Hersher, Rebecca, "Amazon and the $150 Million Typo," NPR The Two Way, March 3, 2017. Accessed August 11, 2024. https://www.npr.org/sections/thetwo-way/2017/03/03/518322734/amazon-and-the-150-million-typo.

[19] CEE Multi-Country News Center. "Major Energy Operator Supports Critical Infrastructure with Cloud Tech," Microsoft. Accessed August 11, 2024. https://news.microsoft.com/en-cee/2021/10/01/major-energy-operator-supports-critical-infrastructure-with-cloud-tech/.

4.6.2. Pacific Gas and Electric Company, California

Pacific Gas and Electric (PG&E) Company, one of the largest electric utilities in the United States, aimed to modernize its grid infrastructure to accommodate the growing number of electric vehicles (EVs) and integrate more renewable energy sources. PG&E leveraged Microsoft Azure's cloud services to modernize its grid for EVs and increase renewable integration. This cloud solution serves as a primary data management system, use case scheduler, and overall control center for vehicle-grid integration (VGI) initiatives. The platform's multifaceted role includes collecting and managing data, translating use case signals across different protocols, interfacing with various aggregators, and tracking the participation of pilot members. PG&E's VGI pilots encompass three distinct programs: a residential pilot, a commercial pilot, and a microgrid pilot. The microgrid pilot is designed to enable bidirectional charging or discharging of EVs within a microgrid, enhancing community resiliency during public safety power shutoff events. The ultimate objective is operational integration with multi-customer microgrids, combining front-of-the-meter microgrids with behind-the-meter support.[20]

4.6.3. Holy Cross Energy, Colorado

Holy Cross Energy, an electric cooperative in Western Colorado, is transitioning to 100% carbon-free electricity by 2030.[21] Emphasizing utility-scale solar, wind, and battery storage, along with local DERs, Holy Cross Energy adopted a cloud-based grid orchestration software platform created by Camus Energy. This platform enhances grid operations by providing real-time visibility, control over member-sited batteries, and access to demand response, resulting in significant cost savings and operational efficiency. Holy Cross Energy envisions becoming a distribution system operator. Holy Cross Energy exemplifies the transformative potential of technology in optimizing grid operations.

4.6.4. GE Vernova, Massachusetts

On February 6, 2023, GE Vernova introduced GridOS, the first comprehensive software suite for grid management. This platform aims to update and enhance the electric grid, making it more resilient and adaptable to clean energy needs. GridOS combines energy data, network modeling, AI, and machine learning to improve grid security and reliability. It helps utilities manage their systems more effectively, aligning IT and OT to meet the demands of a modern energy transition. [22] The platform aims to address the challenges posed by increasing grid complexity, supporting a mission-critical transition to a clean energy grid.

---

[20] National Minority Supplier Development Council. "Pacific Gas and Electric Company Seeking Cloud Platform Provider for Vehicle Grid Integration Pilots," (2023, January 20). Accessed August 11, 2024. https://nmsdc.org/blog/pacific-gas-and-electric-company-seeking-cloud-platform-provider-for-vehicle-grid-integration-pilots/.

[21] Camus Energy, "Blazing a Trail with Holy Cross Energy." Accessed August 11, 2024. https://www.camus.energy/holy-cross-energy.

[22] GE Vernova. "GE Digital Announces GridOS® Software to Help Utilities Orchestrate the Clean Energy Grid and Accelerate the Energy Transition." Last modified: February 6, 2023. https://www.gevernova.com/news/press-releases/GE-Digital-Announces-GridOS-Software.

4.7. Learning Opportunity Case Studies

4.7.1. Australian Electricity Market Operator, Australia

In 2022, Australia experienced a significant electricity distribution disruption when the amount of demand exceeded the electricity supply. Although some electricity was still being sent to end users, the market to regulate distribution and maintain consumption data experienced a breakdown. A key component necessary for consideration in an energy marketplace is electricity to maintain the platform responsible for data and distribution management. For example, investing in alternative energy sources is a questionable business decision if the management resources require the same amount of electricity generated by the alternative energy source. As Australia expands more into the renewable energy sources sector, the intermittence of renewable energy sources, specifically solar and wind, will have to be compensated for through either ESSs or nonintermittent energy systems. The effects of an unstable electricity supply can range from lack of access to necessary household items to loss of life. Figure 3 demonstrates the initial steps in a process that leads to brownouts or blackouts.

When Australia's electricity market failed, distribution, consumption, and generation data was not recorded. This lack of data collection provides concern when cybersecurity and anomaly detection are needed for system security and resilience.

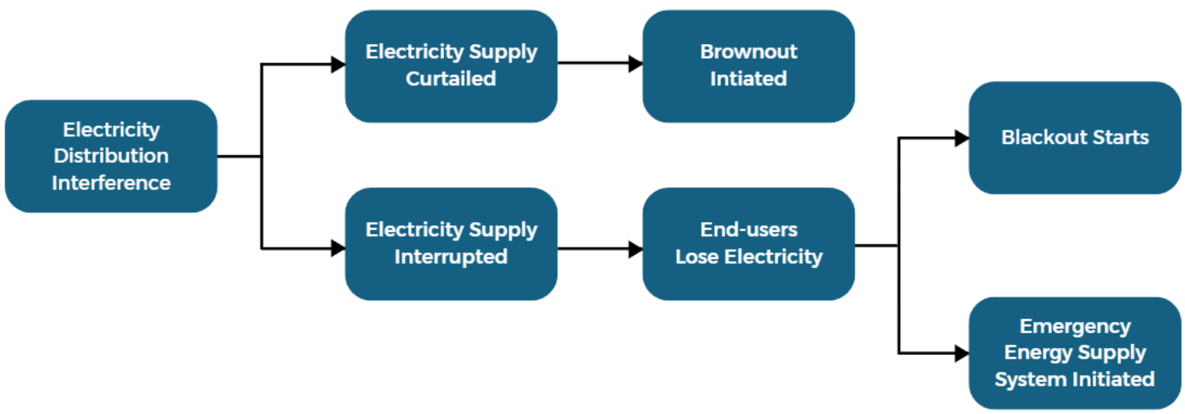

Figure 3. Traditional system processes that lead to brownouts or blackouts.

4.7.2. California ISO, California

Like Australia, California has made strides to decarbonize its state's power grid while electrifying all vehicles sold in the state. This surge in demand, coupled with intermittent renewable energy sources, creates an insecure system susceptible to blackouts caused by various reasons, such as storms, overuse, or cyberattacks. In 2023, California received $67.5 million in federal funding to modernize the grid, which would assist in curtailing blackouts or brownouts.[23] However, California's methodology is marginally complicated by the increased demand for renewably sourced electricity to assist in the decarbonization of the energy infrastructure, coupled with the requirement that all new cars sold in or after 2035 will be EVs. As the energy grid currently exists in California, the infrastructure will not successfully support the dramatic increase in demand associated with the EV policy change. California's insufficient energy infrastructure could require a cultural shift to address the imbalance of supply and demand. An initial, short-term solution for the excess demand is to import renewable energy-sourced electricity from outside sources (i.e., other states). Additionally, intermittent energy sources require an alternative supply to stabilize the supply chain of renewable energy-sourced electric power. Although ESSs are a solution for discontinuous energy supply, they also require regular maintenance and replacement over time, which is a costly temporary solution.

4.7.3. Electric Reliability Council of Texas, Texas

During the winter season of 2021, Texas experienced an excessive amount of power outages that were mostly caused by winter weather events. Unlike most other states in the United States, Texas implements a deregulated electricity market. Though the deregulated electricity market benefits consumers by providing a competitive marketplace to shop for an energy supplier, this alternative marketplace has several disadvantages. Variation in electricity suppliers also means variations in electricity costs based on more sensitive variables. The sensitivity of the market is represented by constantly fluctuating prices. Additionally, the deregulated electricity market increases the complexity of necessary connections between entities participating in the electricity distribution process. This complexity increases the probability of miscommunications, missed maintenance, and overall system malfunction.

5. PROPOSED CLOUD EVALUATION, DEVELOPMENT, AND DEPLOYMENT STRATEGY FRAMEWORK

The following framework and resulting feasibility tool are designed for utility teams considering either a complete transition or an initial cloud application adoption. This framework offers strategic guidance on how to prepare for or deploy a cloud solution responsibly, understanding that each scenario and utility's needs may be unique. The cloud-based risk assessment resource offers utilities a strategic roadmap for adopting cloud technologies. It includes a thorough examination of the utility's risk profile, the anticipated benefits of cloud migration, a readiness assessment, and crucial considerations before and during deployment. These considerations include potential costs, essential questions to pose when evaluating vendors or products, and a comprehensive set of inquiries to guide discussions at each stage. Additionally, it outlines a collaborative process for engaging with other teams within the organization to ensure alignment and successful outcomes.

[23] Padilla, Alex, "U.S. Senator for California, Padilla Announces $67 Million Federal Investment for Grid Resilience in California," July 6, 2023. Accessed August 11, 2024. https://www.padilla.senate.gov/newsroom/press-releases/padilla-announces-67-million-federal-investment-for-grid-resiliency-in-california/.

5.1. Cirrus Framework

Created by the Idaho National Laboratory, Cirrus is a cloud-based tool for electric grid professionals (Figure 4) to assist in the migration process. Cirrus guides users and helps them to navigate the complexities of cloud integration, enhancing operational resilience and efficiency in the electric grid sector. The Cirrus framework, which is the foundation of the tool, uses an adapted version of the Consequence-driven Cyber-Informed Engineering (CCE), Cyber-Informed Engineering (CIE), and the All Hazards Analysis (AHA) approaches to enable responsible and informed decisions.

Figure 4. Cirrus logo and application landing page.

While cloud environments offer scalability, flexibility, and cost-effectiveness, potential security vulnerabilities and performance issues necessitate a thorough evaluation of potential consequences before deployment. The Cirrus framework offers consequence and solution analysis of cloud-based applications for electric grid technologies. Within this decision support framework, an entity can evaluate its most consequential actions from a cloud deployment against tailored and customized engineering metrics such as loss of life, economics, or a power outage. Ranking the consequences for each application creates a quantitative method to develop ECs against and prioritize cloud decisions (i.e., a very high consequence action may not use the cloud, mid-level with low latency needs perhaps uses a hybrid solution, and low consequence proceeds with a cloud solution). The user can also identify the benefits and consequences of not using the new or modernized application. Cirrus aims to facilitate the following for stakeholders:

- **Informed Decision Making**: Cirrus empowers organizations to make decisions based on a thorough analysis of potential consequences and benefits.
- **Risk Mitigation:** By providing tailored engineering metrics, Cirrus aids in mitigating risks associated with cloud deployment.
- **Efficient Cloud Adoption:** Users can efficiently compare implications, ensuring a responsible and informed approach to adopting new or modernized applications.

The cloud integration assessment is a pivotal component of the framework and resulting Cirrus platform, involving the definition of the utility organization, key performance attributes, and risk profile. Cirrus incorporates sliders to assess attributes such as organization size, utility functions, operations technology, current cloud applications, workforce capabilities, and use cases. Figure 5 represents the necessary steps to complete the initial Cirrus survey, which will generate a summarized report.

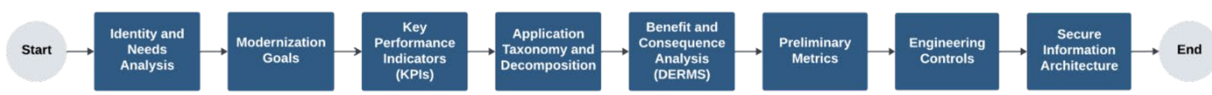

Figure 5. General process followed for completing the Cirrus survey.

The user-provided inputs form the basis for the cloud integration assessment and help develop a tailored cloud strategy. The cloud integration assessment evaluates various aspects of a utility, such as performing identity and needs analysis, identifying modernization goals, key performance indicators (KPI), application taxonomy and decomposition, developing a benefit and consequence analysis, ECs, and secure information architecture. Cirrus offers preliminary metrics, including insights into engineering control applications, secure information architecture, and a high-level report outlining potential organizational measures. The report, provided in PDF format and tailored to user inputs, encompasses a range of elements such as use case taxonomy, mission-critical functions, ADMS apps, deployment size, future cloud options, utility goals priorities, KPI graphs, radar charts, consequence graphs using CCE's high-consequence events (HCEs) equation, request for information (RFI) questions and guidance, and data handling types.

The PDF generated readiness assessment provides the utility with a strategic roadmap for adopting cloud technologies, emphasizing a risk-informed approach to enhance operational resilience and efficiency. The PDF report includes a detailed description of the specific use case, supplemented by taxonomy text boxes that outline key aspects. Mission-critical functions are presented in a bulleted format, while the list of ADMS applications provides insight into deployment size and future cost allocation considerations. The report also addresses the potential transition to the cloud as well as priorities derived from utility goals. Visual representations, such as KPI graphs and consequence graphs, offer further insights (see Figure 6). The HCE graph (shown in Figure 8) leverages the initial CCE-written equation but has been reformulated to provide a given output for Cirrus. The HCE scores are calculated using the equations shown in Figure 7.

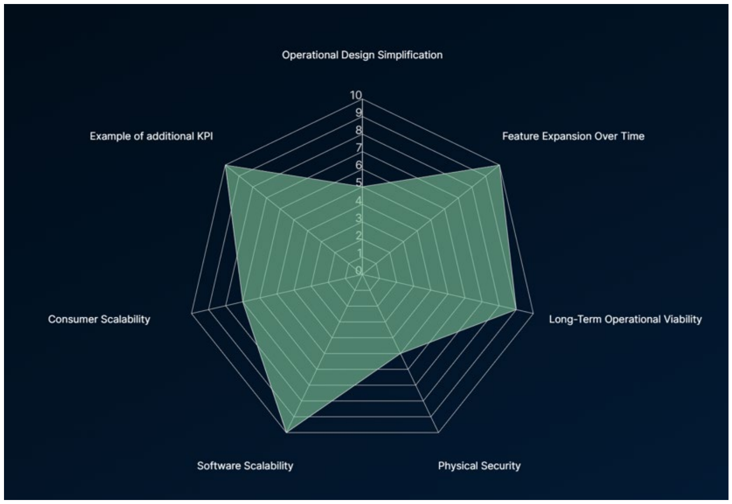

Figure 6. Cirrus KPIs spider chart.

Scored Impact Points

$$\alpha(Area/LoadImpact) + \beta(Duration) + \gamma(Breadth/CascadingImpact) + \delta(Safety) + \epsilon(AssetOwner/SystemIntegrity) + \zeta(Cost)$$

Maximum Impact Points

$$\alpha(3) + \beta(3) + \gamma(3) + \delta(3) + \epsilon(3) + \zeta(3)$$

HCE Severity Score

$$HCESeverityScore = \frac{ScoredImpactPoints}{MaximumImpactPoints} \times 100$$

Figure 7. Cirrus' high-consequence events equations.

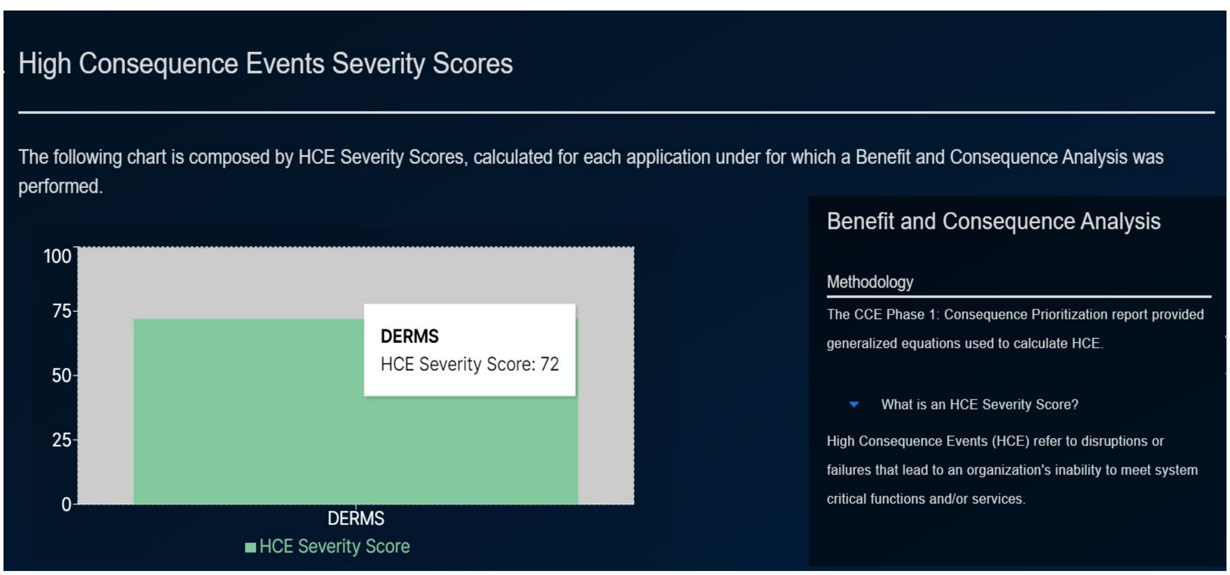

Figure 8. Example of a high-consequence events severity score for DERMs application.

The output of this framework is a profile of the utility's risk, the benefits of cloud migration, the utility's readiness, and considerations—all of which the utility must understand before and during deployment (including potential costs and questions to ask when evaluating vendors or products), along with a key set of questions to ask at each stage and a process to undertake with other teams within the entity.

These questions can be further identified in Appendix B, Framework Requirements and Questions. If it appears the readiness of the entity or user is below where it should be, a set of guidelines on how to increase readiness will be provided, and a reassessment will be performed once those are undertaken.

5.2. Cirrus Calculations and Mapping

The Cirrus framework and tool use specific calculations and mapping to optimize the cloud migration process.

5.2.1. Feature and Key Performance Indicators Evaluation

As shown in Figure 9, Cirrus uses the equations to weigh KPIs on a scale from 0 to 10. Using a failure mode and effects analysis approach, key performance indicators are identified to evaluate systems and system-related processes.[24]

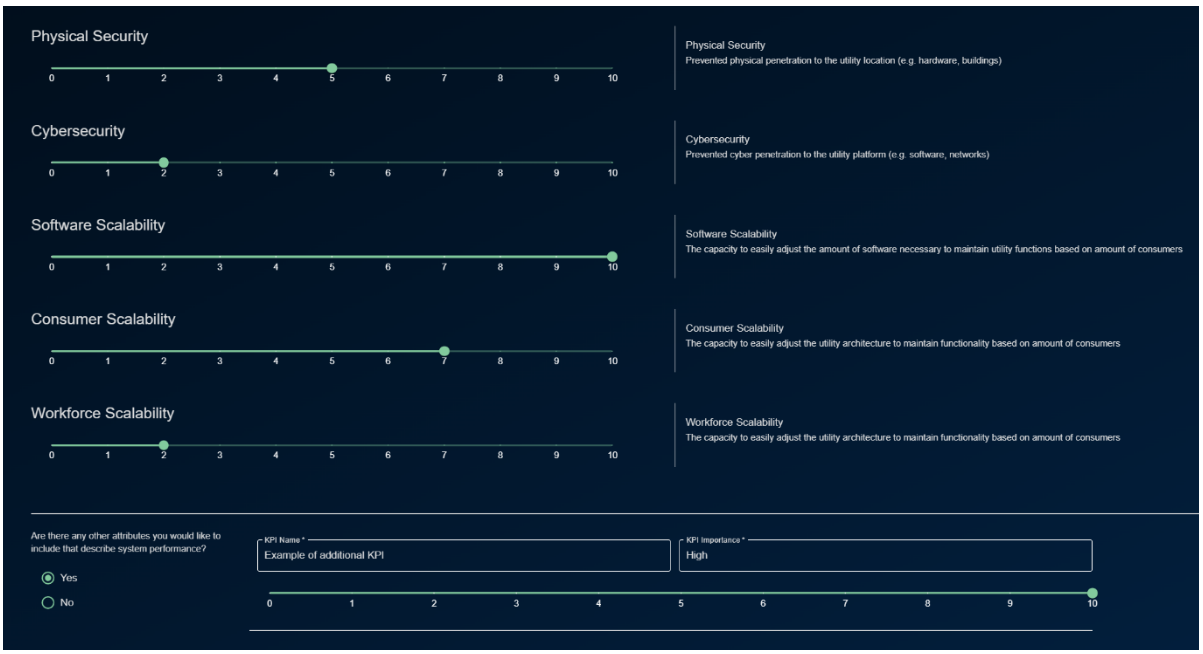

Figure 9. Example of Cirrus KPI chart.

Cirrus identifies a KPI as impactful when its importance is defined as greater than 4. Any KPI with an importance value less than or equal to 4 is disregarded and will not be included in the spider chart viewed on the preliminary metrics page.

5.2.2. Interdependence and Planned Resilience Mapping

The interdependencies shown in Table 2 are summarized from the data input to the framework, and the priority for planned resilience (PR) is calculated from the consequence, latency, and dependencies.

[24] Gillis, Alexander S. and Wendy Schuchart, "Failure Mode and Effects Analysis (FMEA)," Tech Target, December 2022. Accessed August 11, 2024. https://www.techtarget.com/searchcio/definition/FMEA-failure-mode-and-effective-analysis.

Table 2. Interdependencies chart.

Components of Solution	Dependencies				Planned Resilience (PR) (Priority)
	Real-Time Data	Historical – Short	Historical – Long	Other Application Dependency	
FLISR	X	X	X	Geographic Information System (GIS)	Medium - High
Fault Location	—	X	X	GIS, SCADA	Medium
Dynamic Protection	X	—	—	Safety	High
VVC	—	—	X	GIS	Low
SCADA	X	X	X	All	High
Distribution Power Flow	—	—	X	GIS, Asset Management	Low

5.3. Planned Phase 1 Cirrus Components

The Cirrus assessment provides critical outputs for stakeholders to make informed decisions surrounding their cloud migration process.

5.3.1. Output: Report

For an in-depth summary of Cirrus' outcomes, refer to Appendix B. The report deliverable includes the following elements for Cirrus users:

- **Introduction and Use Case Write-Up**
- **Summary of Recommendations**
  - Steps to reduce risk.
  - Recommendations and ideas.
  - Benefits of cloud adoption.
  - Readiness assessment.
- **Consequence Tables and Radar Chart with Description**
  - KPI radar chart.
  - HCE severity scores.
- **Recommended Types of Shared Responsibility Model**

The recommended types of shared responsibility are determined based on the highest consequence and latency requirements of different applications. For example, Table 3 shows which applications are best suited for hybrid, on-premises, and decentralized solutions. By linking data elements to their critical consequences, the table helps establish a clear connection between specific data elements and their potential impacts. This approach ensures that the most critical and latency-sensitive applications are managed in a way that aligns with their specific needs and risks, optimizing the distribution of responsibilities between parties.

Table 3. Cloud model recommendations of components.

Components of Solution	Cloud Model Recommendation			
	On-Premises	Hybrid	Private Cloud	Full Cloud
FLISR	—	X	X	—
Fault Location	—	X	X	—
Dynamic Protection	X	—	—	—
VVC	—	—	X	X
SCADA	X	X	—	—
Distribution Power Flow	—	—	X	X

- **Recommended Request for Proposal (RFP) Questions**
  - Tailored based on styles of requested application, data handling and other.
- **CSP Guidance Based on Inputs** (See Appendix C, How to Select a Cloud Service Provider, for Initial Guide)
- **Recommended Training and Staffing Plans**
  - Suite of potential training, with levels based on scale from calculation of maturity.
- **ECs, Data Security and Handling Summary, and Interdependency Mapping**
- **PR Guide**

5.4. Planned Phase 2 Cirrus Components

The Cirrus framework suggests a phased approach using established strategies and tactics.

5.4.1. Cyber-Informed Engineering-Based Prescriptive Guidance and Template

In Phase 1 of Cirrus, users enter their own discussion on engineering solutions, interdependencies, and resilience. In Phase 2, a prescriptive cybersecurity guide with recommended best practices will be input into the tool to enable users to have a key guide to the actions that can be taken to securely enable their cloud applications and to know the features for which to ask.

5.4.2. Cost Benefit Assessment

Key inputs are defined in the following list to determine the scale of long-term and short-term costs. These inputs are provided as ambiguous terms for a large breadth of applicability. Ambiguity is beneficial for the initial assessment. As a project becomes more defined in purpose, function, and need, assessment factors are defined to fit the unique needs of the organization. Maintaining knowledge and understanding of the benefits of cloud technology changes over time as existing technology develops in an organization.

- Scale of the application: no endpoints, no data inputs, operations vs. planning.
- Decomposition, redundancy, and latency requirements.
- Data classification, residency, and retention requirements.
- Future cloud and modernization goals and load or endpoint growth.
- Business drivers.

Using each of these features, a projected cost scale is developed, with weights to show the user things that will increase and decrease cost over time. This costing is plotted with the business drivers and their potential benefits in Table 4.

Table 4. Top business drivers and solution components.

Components of Solution	Top Business Drivers				Cost Short Term	Cost Long Term
	Reliability Metric	Cost Savings	Resilience	Scalability		
FLISR	—	X	X	—	$	$$
Fault Location	—	X	X	—	$$	$$
Dynamic Protection	—	—	—	—	$$$$	$$$$$$
VVC	—	—	—	—	$	$$$
SCADA	—	—	—	—	$$$$	$$$$$$
Distribution Power Flow	—	—	X	X	$	$$$

5.4.3. Additional Use Cases

ADMS is the first use case developed. ADMS is a series of applications. Therefore, multiple use cases within this are now developed. Additional use cases that will be outlined include the following:

- Asset management and predictive maintenance
- Smart metering and AI/Enhanced data analytics
- DERMS
- Data management and planning tools.

5.4.4. Trend Tracking

Over time, as users enter more information on the applications, benefits, and challenges, this data (anonymized and aggregated) will be used to validate and further a gap and cloud trend analysis for the electric industry.

5.4.5. Cloud Service Mapping and Cloud Service Provider Selection

Based on the input given and industry outreach, the specification entered will be used to map a capability chart for the large CSPs against the requirements of these applications.

6. SUMMARY AND CONCLUSIONS

Cloud adoption offers utilities scalability, flexibility, and cost-effectiveness, empowering them to focus on core business activities while offloading server management to IT professionals. By leveraging cloud technology, utilities can enhance their IT and OT capabilities, streamline operations, and adapt to new digital applications rapidly. Third-party integrators, software vendors, and hardware vendors facilitate cloud adoption, offering specialized solutions tailored to the unique needs across critical infrastructure sectors, including energy, communications, water, and transportation. Cloud-based architectures can offer resilience, connectivity, and efficiency, which are essential for managing DERs and ensuring uninterrupted service delivery.

However, this transition is not without challenges, particularly regarding security and shared responsibility. With careful planning and consideration of the insights and framework provided, utilities can make well-informed decisions regarding cloud implementation that align with their unique needs and objectives. One approach is implementing the Cirrus software, which serves as a valuable tool, offering utilities strategic guidance and support for responsible cloud adoption. Through the utilization of Cirrus, utilities can conduct assessments and implement adaptable frameworks, ensuring judicious decision-making and proficient risk management throughout the cloud deployment process.

7. REFERENCES

Garton, D. 2019. “Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation.” National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure, November 12, 2019. https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf.

Department of Homeland Security. n.d. “Critical Infrastructure.” Accessed August 9, 2024. https://www.dhs.gov/science-and-technology/critical-infrastructure.

Rinaldi, S. M., J. P. Peerenboom, and T. K. Kelly. 2001. “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies.” *IEEE Control Systems Magazine* 21(6): 11–25.

ABI Research. 2023. “With COVID-19 Behind, New Cybersecurity Spend in Critical Infrastructure to Reach US$236 Billion by 2027.” Accessed August 9, 2024. https://www.abiresearch.com/press/with-covid-19-behind-new-cybersecurity-spend-in-critical-infrastructure-to-reach-us236-billion-by-2027/.

Younis, Y. A., M. Merabti, and K. Kifayat. 2013. “Secure Cloud Computing for Critical Infrastructure: A Survey.” In proceedings of the 14th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking, and Broadcasting, 599–610.

Enel Group. 2019. “Enel 'Full Cloud': All the Advantages of Being the Pioneers.” Accessed August 9, 2024. https://www.enel.com/company/stories/articles/2019/07/enel-moves-cloud-model-future.

Duke Energy Corporation. 2022. “Duke Energy Collaborates with AWS to Develop Smart Grid Solutions to Better Serve Customers and Drive its Clean Energy Transition.” Accessed August 9, 2024. https://news.duke-energy.com/releases/duke-energy-collaborates-with-aws-to-develop-smart-grid-solutions-to-better-serve-customers-and-drive-its-clean-energy-transition.

National Grid. n.d. “Driving our Digital Transformation.” Accessed August 11, 2024. https://www.nationalgrid.com/digital.

Rooney, P. 2022. “National Grid’s Energy Transformation is Fueled by IT.” CIO, Accessed August 11, 2024. https://www.cio.com/article/350316/national-grids-energy-transformation-is-fueled-by-it.html.

Vestas. n.d. “Digital Services.” Accessed August 11, 2024. https://www.vestas.com/en/energy-solutions/service/digital-services.

Contino. n.d. “Accelerating Innovation and Cloud Adoption at EDF with a Cloud-Native Landing Zone and Operating Model in Just Ten Weeks.” Accessed August 11, 2024. https://www.contino.io/case-studies/EDF-Cloud-Adoption.

Orsted A/S. n.d. “Building More Than Ever Before.” Accessed August 11, 2024. https://orsted.com/.

E.On. n.d. “E.ON Ectocloud: Intelligent Control.” Accessed August 11, 2024. https://www.eon.se/en_US/foeretag/ectogrid/ectocloud.

National Telecommunications and Information Administration, n.d. “Broadband Equity Access and Deployment Program.” United States of America Department of Commerce, Accessed August 11, 2024. https://broadbandusa.ntia.doc.gov/funding-programs/broadband-equity-access-and-deployment-bead-program.

Hersher, R. 2017, “Amazon and the $150 Million Typo.” NPR, The Two Way. Accessed August 11, 2024. https://www.npr.org/sections/thetwo-way/2017/03/03/518322734/amazon-and-the-150-million-typo.

Liberty-NH. 2019. “Distribution Line Overarching Strategy.” New Hampshire Public Utilities Commission. Accessed August 11, 2024. https://www.puc.nh.gov/Regulatory/Docketbk/2019/19-120/TESTIMONY/19-120_2019-12-04_GSEC_ATT_REV_TESTIMONY_JOHNSON_RIVERA_STRABONE_TEBBETTS.PDF.

CEE Multi-Country News Center. 2021. “Major Energy Operator Supports Critical Infrastructure with Cloud Tech.” Microsoft. Accessed August 11, 2024. https://news.microsoft.com/en-cee/2021/10/01/major-energy-operator-supports-critical-infrastructure-with-cloud-tech/.

National Minority Supplier Development Council. 2023. “Pacific Gas and Electric Company Seeking Cloud Platform Provider for Vehicle Grid Integration Pilots.” Accessed August 11, 2024. https://nmsdc.org/blog/pacific-gas-and-electric-company-seeking-cloud-platform-provider-for-vehicle-grid-integration-pilots/.

Camus. n.d. “Blazing a Trail with Holy Cross Energy.” Accessed August 11, 2024. https://www.camus.energy/holy-cross-energy.

GE Vernova. 2023. “GE Digital Announces GridOS® Software to Help Utilities Orchestrate the Clean Energy Grid and Accelerate the Energy Transition.” Accessed August 30, 2024. https://www.gevernova.com/news/press-releases/GE-Digital-Announces-GridOS-Software.

Padilla, A. 2023. “Padilla Announces $67 Million Federal Investment for Grid Resilience in California.” Accessed August 11, 2024. https://www.padilla.senate.gov/newsroom/press-releases/padilla-announces-67-million-federal-investment-for-grid-resiliency-in-california/.

Gillis, A. S., and W. Schuchart. 2022. “Failure Mode and Effects Analysis (FMEA).” Tech Target, Last updated December 2022. Accessed August 11, 2024. https://www.techtarget.com/searchcio/definition/FMEA-failure-mode-and-effective-analysis.

Appendix A

Framework Development References

Cloud Security Alliance. 2018. "Cloud Security Alliance Announces FedSTAR, a New Joint Certification System with FedRAMP." Accessed August 9, 2024. https://cloudsecurityalliance.org/articles/cloud-security-alliance-announces-fedstar-a-new-joint-certification-system-with-fedramp/.

Cloud Security Alliance. n.d. "Security, Trust, Assurance and Risk (STAR)." Accessed August 9, 2024. https://cloudsecurityalliance.org/star/.

Federal Risk and Authorization Management Program (FedRAMP). Accessed August 9, 2024. https://www.fedramp.gov/.

International Organization for Standardization (ISO). 2022. "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements." Accessed August 9, 2024. https://www.iso.org/isoiec-27001-information-security.html.

Joint Task Force Transformation Initiative. 2013. "Security and Privacy Controls for Federal Information Systems and Organizations." NIST Special Publication (SP) 800-53, Revision 4, 2013. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

Mell, P., and T. Grace. 2011. "The NIST Definition of Cloud Computing." NIST Special Publication (SP) 800-145, Gaithersburg, MD. Accessed August 9, 2024. https://doi.org/10.6028/NIST.SP.800-145.

Iorga, M., and A. Karmel. 2016. "Managing Risk in a Cloud Ecosystem." *IEEE Cloud Computing Magazine* 2(6): 51–57. https://doi.org/10.1109/MCC.2015.122.

Microsoft. n.d. "What is SaaS?" Accessed August 9, 2024. https://azure.microsoft.com/en-us/overview/what-is-saas/.

Microsoft. "Azure Homepage" Accessed August 9, 2024. https://azure.microsoft.com/en-us/.

National Institute of Standards and Technology (NIST) 2018. "Framework for Improving Critical Infrastructure Cybersecurity." NIST Cybersecurity Framework, Version 1.1. Accessed August 9, 2024. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

National Institute of Standards and Technology (NIST). 2004. "Standards for Security Categorization of Federal Information and Information Systems." FIPS PUB 199, Accessed August 9, 2024. Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.

North American Energy Standards Board (NAESB). n.d. *NAESB Homepage*. Accessed August 9, 2024. https://www.naesb.org/.

North American Electric Reliability Corporation (NERC). n.d. "Supply Chain Risk Mitigation Program." Accessed August 9, 2024. https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

Oracle. "Network Management System Configuration Guide." Last modified April 17, 2024. https://docs.oracle.com/cd/E98860_01/PDF/NMS_V2_4_0_0_Configuration_Guide.pdf.

SDxCentral Studios. n.d. "What are Cloud Service Providers?" Last updated November 2020. Accessed August 9, 2024. https://www.sdxcentral.com/cloud/definitions/what-are-cloud-service-providers/.

United States Computer Emergency Readiness Team (US-CERT). n.d. "Meltdown and Spectre Side-Channel Vulnerability Guidance." U.S. Cybersecurity & Infrastructure Security Agency. Last revised May 1, 2018. Accessed August 30, 2024. https://www.us-cert.gov/ncas/alerts/TA18-004A.

Appendix B

Framework Requirements and Questions

The approach is based on INL's Cyber-Informed Engineering (CIE) framework and industry-informed input and references other established commercial frameworks. The Cirrus model works through multiple stages, including:

1. Understand who is inputting information and assess their current profile regarding modernization and risk.
2. Define applications and future plans, including the organization's risk tolerance.
3. Evaluate the consequences and benefits of the applications and deployments being considered, enabling prioritization of mitigations and solutions to challenges.
4. Step through a series of questions and controls to form a capability profile.
5. Summarize key issues to facilitate the transition (if needed).

Step 1: Identity and Needs Analysis

This step covers questions on the following:

- Utility Size
- Business Model
- Transmission and Distribution
- OT Status
- Cloud Application(s) Status
- Information Technology (IT) Staffing
- Amount of IT Staff
- Use of MSP or MSSP
- Applications
- Customer Base
- Endpoints
- Modernization goals

Step 2: Consequence Analysis, Application Decomposition, and Taxonomy Development

This step allows a utility to classify systems within their utility by assessing the following:

- Purpose of proposed system
- Organizational support
- Existing system processes
- Consequences if failure occurs

Step 3: Develop ECs Around the Site

This step highlights applications with higher risk severity scores by inquiring the following:

- For the highest consequence applications score, are there engineering control mitigations that would reduce the risk?
  - Hybrid cloud approach
  - Local controls
  - Low-latency fiber
  - No
- For the middle consequence applications score are there engineering control mitigation that would reduce the risk?
- What is the scale of the cost of those controls in addition to the cost of the application to the cloud?
- Does it mitigate the risk? (A very low latency dedicated fiber for protection that runs to the cloud is expensive, does the financial benefit or benefit of doing the application overall balance out the cost)
- What is the benefit of the additional controls?
- Are there additional benefits that could be considered by having a specific control (e.g., additional data from the low-latency high-throughput fiber)?

Step 4: Secure Information Architecture and Digital Asset Management Planning Evaluation and Consideration

This step helps utilities develop a plan of what data is important based upon the classification of that data, and access requirements by asking the following:

- What type of data will be in this system?
  - Critical energy/electric infrastructure information (CEII)
  - Business sensitive information
  - Personally identifiable information (PII)
  - Operations models
  - Geographic Information System (GIS)
  - Planning models
  - Protection settings
  - Intellectual property (IP)
  - Health information (HIPAA)
  - Financial data (PCI DSS)
  - Government classified information
- What is the minimum viable set of information that must be released for system design and to whom must it be released?
- Data Residency: Requirement for data classification above where it must live.
- Do you require consent before data is moved?

Step 5: Simplification and Interdependency

Data Interdependency Questions:

- Which data flows are needed from other on-premises systems?
- Which data flows are needed from other cloud systems?
- Which public data are needed?

- Which applications depend on onsite communications?
- How much data is needed on-premises to operate the most consequential, low-latency applications?
- Identify essential features for the cloud deployment, explore the possibility of reducing features to mitigate risks, and determine the most crucial aspects within the device.
- During an emergency, which applications must operate, and which applications can be degraded or run without communications or data?
- Determine (if known) the ingress and egress points for all data.
- Assess operational elements required for the application from other systems and their speed of integration, guided by the original table.

Step 6: Evaluate Digital Asset Awareness and Develop Cyber-Secure Supply Chain

Assessment of asset inventory.

- List all hardware, software, network, and data storage solutions.
- Catalog custom and commercial solutions.

Step 7: Develop a Planned Resilience (PR) and Operations Model

Consider the development of diminished operating modes with limited communication limited critical function support.

- What can be diminished over time?
- What does not need fast communications?
- Can you transition to cloud or hybrid approach some functions?

Step 8: Current Security Posture, and Developing a Resilient Layered and Active Defense Model for New and Existing Applications

Determine the best compilation of defenses and mitigations from the extensive solution environment to provide the most coverage and defense from critical consequences.

The steps to understanding the needs modeling a resilient defense for the system include the following:

- Evaluate staffing and a security list of requirements.
- Determine any regulatory concerns or compliance issues.
- Determine current security posture (small assessment).
- Determine future required or desired posture.
- Determine site needs to get to the required or desired posture.
- What sort of training is provided for current employees?
- Who will be responsible overall for the cloud posture?

Appendix C

How to Select a Cloud Service Provider

C-1. Phase 1: Build the Justification and Assessment Framework

Establish Business Justification: Clearly define the goals and expected benefits of cloud adoption for your utility. Quantify potential cost savings, operational efficiencies, and other value drivers.

- Develop Bid Model Criteria: Create a comprehensive list of criteria against which you will evaluate potential Cloud Service Provider (CSPs).
- Information Technology and Non-Regulated Requirements: Consider offerings such as drone video storage, assessing data privacy, and security risks.
- Cost Management: Align cloud costs with rate case approvals and Public Utility Commission regulations.
- Integration and Transition: Evaluate seamless integration with existing technology infrastructure and support for smooth transitions.
- Telecom Infrastructure: Assess bandwidth and resiliency needs for various use cases (e.g., site-to-site, local area network, edge devices) and explore alternative data paths.
- Compliance: Ensure adherence to all relevant industry regulations and security standards.

C-2. Phase 2: Select the Optimal Cloud Solution

- Perform Assessment: Implement the established framework to evaluate potential CSPs against the predefined criteria. Gather detailed information and proposals from each vendor.
- Identify Cloud Architecture: Use the gathered information to define the most suitable cloud architecture for your specific needs. Consider scalability, flexibility, and alignment with future growth plans.
- Select Cloud Service: Choose the CSP that best meets your requirements based on the assessment, considering factors like security, reliability, and cost-effectiveness.
- Gain Visibility and Negotiate Risks: Conduct a thorough review of the chosen cloud offering, focusing on risk management and control measures. Define and negotiate necessary risk mitigations before finalizing the service-level agreement (SLA) and securing authorization.

C-3. Phase 3: Ongoing Secure Cloud Operations

- Identify Security and Privacy Controls: Map out all cloud-specific risk-adjusted security and privacy controls required for your operations.
- Secure Service Agreements: Obtain contractual agreements and SLAs from the CSP and any involved brokers, clearly outlining their responsibility for implementing and maintaining designated security and privacy controls.

- Assess Control Implementation: Conduct regular audits and assessments to verify the ongoing implementation of agreed-upon security and privacy controls by the CSP.
- Continuous Monitoring: Establish a robust monitoring system to track and maintain awareness of any changes or vulnerabilities within the cloud environment, ensuring constant compliance and optimal security posture.

C-4. Additional Specific Considerations

- Industry-Specific Regulations: Emphasize compliance with relevant regulations, such as NERC CIP and FERC, for secure electricity grid operations.
- Data Governance and Privacy: Prioritize robust data governance policies and protocols to safeguard sensitive customer and operational data.
- Vendor Lock-In: Minimize dependence on specific vendors by implementing open standards and portable solutions.
- Infrastructure Evaluation: Utilities must first audit existing IT and OT infrastructure to determine the feasibility of integrating with cloud services. This includes an assessment of legacy systems and their compatibility with cloud platforms.
- Regulatory Compliance and Security: Given the critical nature of utilities, compliance with regulatory standards, such as NERC CIP, is crucial. The assessment should include a gap analysis of current cybersecurity measures against cloud-provider offerings to ensure data protection and privacy.
- Workforce Capability: The utility's workforce must be equipped with the necessary skills for a smooth transition. This involves evaluating current staff expertise and identifying areas where additional training or hiring is necessary.
- Operational Resilience: Utilities should assess their capacity to maintain operations during the migration phase and potential cloud outages. This includes evaluating disaster recovery and incident response plans in a cloud-based environment.
- Cost-Benefit Analysis: A thorough financial analysis is essential to justify the investment in cloud migration. Utilities must consider not only the upfront costs but also the long-term operational savings and potential for innovation.
- Vendor Selection: When selecting a CSP utilities must consider factors such as SLAs, support for the energy sector, and the ability to provide hybrid cloud options that can cater to their specific needs.

C-5. Example of Request for Proposal Questions

The following is a comprehensive set of guidelines that can serve as a roadmap for developing data management for application deployment and working with an request for proposal (RFP). These guidelines encompass strategic considerations for sharing information with vendors, network segmentation, cloud service utilization, personnel access requirements, and a nuanced approach to tying data elements to critical consequences.

Sharing Minimum Viable Information with Vendor:

- Limit sharing to design specifications, information, and communications architecture.
- Restrict sharing of nonessential equipment types for design and operation.

Segmentation of Operational Network:

- Segment the operational network into three distinct zones: enterprise, control centers, and substations with Demilitarized Zone.
- For each segment, identify need to know, association, and aggregate impact.
- Classify datasets and evaluate the consequences of placing them on the cloud in aggregate.
- Implement a number metric to assess the level of security and compliance.

CEII Identification and Cloud Services:

- Identify clouds capable of providing CEII.
- Ensure data segregation for storage and controlled access within cloud applications.

Requirements for Personnel Accessing Data:

- Specify data residency requirements.
- Specify the country where data is located and establish controls to prevent unauthorized data movement.

Data Handling Guidance for Cloud Applications:

- Address security measures, encryption, and access controls to ensure data integrity.