[INL/RPT-24-81423]

Enhancing Cloud Cybersecurity: Prescriptive Controls for Operational Technology

White Paper

October 2024

Emma Stewart, Julia Morgan, Nathan Woodruff, Glenn Combe 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

Enhancing Cloud Cybersecurity: Prescriptive Controls for Operational Technology

White Paper

Error! Not a valid bookmark self-reference.

Idaho National Laboratory
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

TABLE OF CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

CIE	Cyber-Informed Engineering
DER	Distributed Energy Resources
IaaS	Infrastructure as a Service
IoT	Internet of Things
IT	Information Technology
MSSP	Managed Security Service Provider
OT	Operational Technology
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
SaaS	Software as a Service

Page intentionally left blank

EXECUTIVE SUMMARY

This whitepaper provides strategic insights and recommendations into security cloud-based solutions for electric utilities, encompassing operational technology (OT), virtual power plants (VPP), distributed energy resources (DERs), applications, networks, and data storage as they transition to and leverage cloud infrastructure through managed service providers (MSPs) and cloud service providers (CSPs). Principles derived from established frameworks serve as a foundation for best practices across cybersecurity projects and remove the constraints of settling on a single framework. For organizations that prefer not to integrate a specific framework altogether, elements of the proposed approach could be adopted or tailored to best fit defined requirements and expected functionalities.

The Cirrus assessment, a utility cloud feasibility tool, and the roadmap it provides serve as a precursor to this paper, which seeks to be a valuable resource for defining next steps following cloud technology integration feasibility appraisal. With its comprehensive approach to adoption, the Cirrus framework offers strategic guidance on responsibly preparing for or deploying a utility cloud solution. The previously published whitepaper, "Use Case-Informed Framework for Utility Cloud Migration," details the guiding strategy, research, and deployment of cloud solutions within electric and interconnected grid systems. Before implementing the controls suggested in this document, it is recommended that stakeholders complete Cirrus's cloud integration assessment and pair the results with their unique cybersecurity controls to form a comprehensive cloud-based utility cybersecurity plan. The Cirrus outcome will consider a series of future architectures for the grid before and after the energy transition and evaluate the arguments for and against cloud applications for each electric and interconnected grid layer. This document is a companion to the original whitepaper to further identify and recommend security controls based on Cirrus's cloud integration assessment output.[1]

The following whitepaper outlines the cybersecurity controls that secure cloud-service models pertinent to the electric sector using the predefined categories identify, protect, detect, and respond and recover. The objective is to outline prescriptive security controls based on the type of architecture and data stored in the cloud. The focus includes dissecting the shared responsibility model and elucidating what on-premises Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) entail. A pivotal consideration in this context is allocating responsibility for foundational cybersecurity aspects—having used Cirrus for the cloud integration assessment. The ensuing controls detailed herein also represent a checklist of controls necessary for a secure cloud transition, equipping utilities with the knowledge to navigate this digital transformation with confidence and strategic foresight in a safe and responsible manner.

Error! Reference source not found.

INTRODUCTION

As cloud computing has grown and matured over the last decade, there has been a transformative shift across various industries, with the energy sector at the forefront of this revolution. Utilities, traditionally reliant on robust in-house physical infrastructures with Information Technology (IT) and Operational Technology (OT), are now pivoting towards the cloud and digitized services for enhanced data management, email communications, and business operations. Additionally, there is contemplation about transitioning operational and control functions to the cloud. Smaller utilities, often lacking robust IT and OT infrastructures, are considering cloud technology as a swift solution for modernization. The allure lies in access to powerful computing resources and, importantly, SaaS offerings providing ready-made solutions for managing and optimizing decisions with vast amounts of data.

Stakeholders should carefully consider leveraging the cloud for utility-based cloud-native operations and hybrid model operations that extend existing physical infrastructure and new cloud-based capabilities. Not only are there different defined models of responsibility based on the SaaS, IaaS, and PaaS models the cloud offers for operation, but also various types of cloud offerings in terms of security controls. It is also recommended that private cloud solutions be employed when transitioning energy-related operations, applications, distributed energy resources (DERs), advanced encryption standards (AESs), and supporting systems to the cloud, ensuring ownership and security solely by the implementing entity. Shared and community cloud options should be avoided due to potential risks associated with resource sharing, the sensitivity of data, and its impact on operations.

The impetus behind a universal cloud-computing migration is multifaceted. The changing mix of energy resources requires skilled and complex management of widespread systems. Also, the common use of digital technology and microprocessor devices highlights the importance of using cloud-based solutions. Many of these devices automatically send data to the internet for processing by the vendor. In some situations, access through a vendor portal is the only way a user can view specific data. In other cases, vendors using the data for health monitoring may void warranty agreements if cloud connections are cut. Cloud services offer models for resilience with geographic redundancy and geographic dispersion, essential in facing challenges akin to those witnessed in Texas, California, Ukraine, and regions prone to severe weather.[2] Furthermore, the utility sector optimizes advanced analytics and artificial intelligence in its decision-making and integrates new product choices, such as advanced distribution-management systems (ADMSs), creating further cloud-computer adoption trends in other sectors. This approach increasingly limits access to in-house solutions.[3]

Cloud computing also presents a compelling economic proposition, enabling utilities to manage costs effectively and concentrate on core business activities by offloading server and hardware administration to IT professionals who can ensure secure network management. However, this transition is not without its challenges, particularly in the realms of security and shared responsibility. Ineffective management can lead to escalating costs. Thus, a thorough evaluation and a scalable analytical framework are imperative to mitigate potential obstacles.

A cloud migration trend is gaining momentum across various sectors. Within the utility sector, the transition manifests in diverse forms that require a slightly varied approach to cyber security from traditional IT data and networks. With availability being the driver of the networks and confidentiality and integrity secondary tenants to availability and resilience, many of the same tenants apply to the Cloud of Things (CoT) and OT, but there are some distinctions. These strategies impact how utilities effectively identify efficiencies, protect against threats or malfunction, detect threats or malfunction, and respond and recover quickly to challenges utilizing cloud computing mechanisms.

IDENTIFY

Identifying the cloud computing needs of utility and electrical companies is imperative because it ensures the optimization of cloud technology deployment to enhance operational efficiency, resilience, and security. By comprehensively understanding their specific requirements, these entities can engineer bespoke cloud solutions tailored to manage data more effectively, optimize decision-making processes, and address unique challenges such as the integration of distributed energy resources and advanced analytics. Furthermore, a well-articulated cloud strategy is instrumental in mitigating risks, reducing operational costs, and maintaining regulatory compliance, thereby contributing to a more reliable and sustainable energy infrastructure.

About Cirrus

Cirrus is a tool developed at the Idaho National Laboratory (INL) that provides a comprehensive cloud feasibility and integration assessment, guiding users through the complexities of cloud integration (Figure 1). By completing the assessment and following the strategic roadmap developed outlining the organization's unique needs, the entity can expect enhanced operational resilience and efficiency in the electric grid sector. Cirrus integrates multi-criteria decision-making and risk assessment to provide the user with risk-informed solutions, aiding in cloud technology implementation.

Figure 1: Cirrus' homepage.

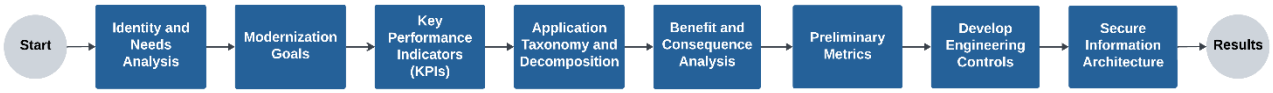
The Cirrus framework uses an adapted version of the Consequence-driven Cyber-informed Engineering (CCE), and Cyber-informed Engineering (CIE) approaches that, when integrated, enable responsible and informed decisions. CIE is leveraged within the Cirrus application from an IT-driven perspective, focusing on the implementation of cybersecurity measures within cloud infrastructure. CIE is leveraged throughout the Cirrus framework to embed cybersecurity considerations at the foundational levels of design and operation. CIE, as defined herein, emphasizes the integration of security principles and practices into the engineering processes of cloud-based systems to mitigate cyber risks effectively. CCE is used to enhance existing cybersecurity tools and strategies. Risk management strategies suggested by the Cirrus assessment are based on consequence prioritization of organizational values. Additionally, mitigation strategies offer protective measures to the most critical vulnerabilities and are identified as opportunities for the organization to focus on during cloud implementation.

The Cirrus framework provides a structured approach to evaluating the implications of deploying cloud-based applications for electric grid technologies. It assesses potential consequences and solutions to aid in decision-making, risk mitigation, and efficient cloud adoption. The Cirrus portal provides consequence and solution-based analysis by evaluating cloud deployment actions against customized engineering metrics such as loss of load, economic impacts, and power outages. Ranking the consequences for each application guides decisions on whether to use cloud solutions, hybrid solutions or avoid cloud deployment altogether. This framework facilitates informed decision-making by thoroughly analyzing potential consequences and benefits to enable data-driven decisions.

Cirrus' Cloud Risk Assessment

Risk mitigation is a core component of Cirrus, utilizing tailored engineering metrics to help mitigate risks associated with cloud deployment. Using the assessment tool ensures efficient cloud adoption by comparing implications and promoting a responsible approach to adopting new or modernized applications. The Cirrus cloud integration assessment defines organization-specific attributes, performance metrics, and risk profiles. The outcome is a PDF report that includes visualizations of Key Performance Indicators (KPIs), a consequence matrix used for risk analysis, and a strategic roadmap that outlines critical milestones throughout the cloud implementation process with associated risks. As shown in Figure 2, Cirrus incorporates identity and needs analysis, modernization goals, key performance indicators, application taxonomy, and benefit and consequence analysis. Preliminary metrics, insights into engineering control applications, and a high-level report outlining potential organizational measures are provided.

Figure 2: Cirrus' steps within the cloud integration assessment.



Cirrus also utilizes a consequence graph, which visualizes the severity of potential events, allowing organizations to prioritize mitigation strategies based on the most critical risks. This tool aids in making informed, data-driven decisions by clearly showing the impact of various scenarios.

Figure 3: Example of Cirrus' HCE output.

Figure 3 features a visual representation of the Cirrus consequence graph, which is calculated using the High Consequence Events (HCE) equations. The HCE score is visualized on a horizontal bar graph,

where the higher score represents the more severe consequences of the event(s). The report also offers pre-populated request for information (RFI) questions, guidance on data handling types, and a consequence matrix for risk analysis. It delivers a profile of the utility's risk, benefits of cloud migration, readiness, potential costs, and vendor evaluation questions.

Cirrus' Evaluation Concepts

Eight evaluation concepts are identified in the Cirrus framework. They include understanding the utility's operational identity and data footprint to determine cloud needs; assessing current IT and OT infrastructure and cloud migration necessity; evaluating the business model and structure of the utility; determining the workforce's capability and size for supporting cloud migration and operations; reviewing existing network management strategies and cybersecurity measures; and integrating preliminary metrics and insights into engineering control applications. Further steps involve high-level reporting on potential organizational measures such as readiness assessment, risk management, and strategic objectives alignment for effective cloud integration. Each evaluation criterion adds value to the Cirrus assessment and its application to cloud migration.

1. Preliminary Analysis and Foundational Information

Utilities must first understand their operational identity and data footprint. This can be used to determine their unique cloud needs based on the type of energy system and their ability to be cloud integrated. This analysis involves a thorough assessment of current capabilities, infrastructure, and strategic objectives to align cloud services accordingly. The "Identity and Needs Analysis" component establishes who the user is and assesses their readiness and maturity for the transition (by determining the level of security, utility, staffing, and current cloud posture). To evaluate readiness for cloud migration, the Identity and Needs Analysis assessment section provides an evaluation of the aspects below and then applies the resulting information to the assessment steps that follow:

- **Cloud Migration Needs:** Assesses the current IT and OT infrastructure states and the necessity of migrating to the cloud.
- **Business Model and Structure:** Determines the utility type and operational model.
- **Staffing and Size:** Determines the workforce's capability and size to support cloud migration and ongoing operations or the need for third-party management.
- **Current Network Management Strategy and Maturity:** Reviews the existing strategies for managing the network, including cybersecurity measures and operational protocols.
- **Modernization Strategy:** Improves resilience and operations by integrating distributed energy resources (DERs).
- **Determine End Points and Customer Base:** Scales the estimated cost of new applications.
- **Preferences and Required KPIs:** Identifies system performance needs.

The identification and needs assessment steps are foundational for utilities to understand their current position and plan accordingly for a transition to cloud services, considering their ideal organizational future. The readiness assessment will culminate in a detailed report (further detailed in the Appendix) that outlines the strategic roadmap for cloud migration, highlighting the potential benefits, the risks involved, and the steps required to ensure a successful transition.

2. Consequence Analysis, Application Decomposition, and Taxonomy Development

The second Cirrus evaluation area focuses on identifying key applications and how their components are broken down to recognize enabling features that guide the selection of cloud services. The assessment begins with a detailed evaluation of critical functions and potential consequences. This includes analyzing the physical and cybersecurity performance of essential systems, considering factors such as safety, grid impact, equipment integrity, and broader systemic implications. The "Consequence Analysis" assessment section focuses on the following aspects:

- **Application Failure Consequence**: Evaluates the system's critical functions and the undesired consequences that must be prevented.
- **Consequence Prioritization:** Focuses on risk management and select operations that must not fail and the associated cloud failure scenarios that could bring them down (both cloud and not cloud-related), along with the benefit(s) of these applications. The following questions are used to evaluate the benefit(s) of application success:
    1. What is the purpose of the proposed system?
    2. How does it support the organization?
    3. What system processes exist already for the function?
    4. What happens when they fail?
    5. What happens when they are improved?
    6. What mission-critical functions must this system provide or ensure?
    7. What undesirable consequences should it prevent?

The utility's operational electricity demands, such as the frequency of application usage and required roundtrip execution times, are evaluated to determine cloud service specifications. Each function is analyzed for its key business drivers, including area/load impact, duration, safety, and cost. Table 1 demonstrates the weighting of the impact that is created in the application to determine the priority of the application's consequences being considered. Figure 4 below shows an example of Cirrus' consequence matrices generated for DERMS.

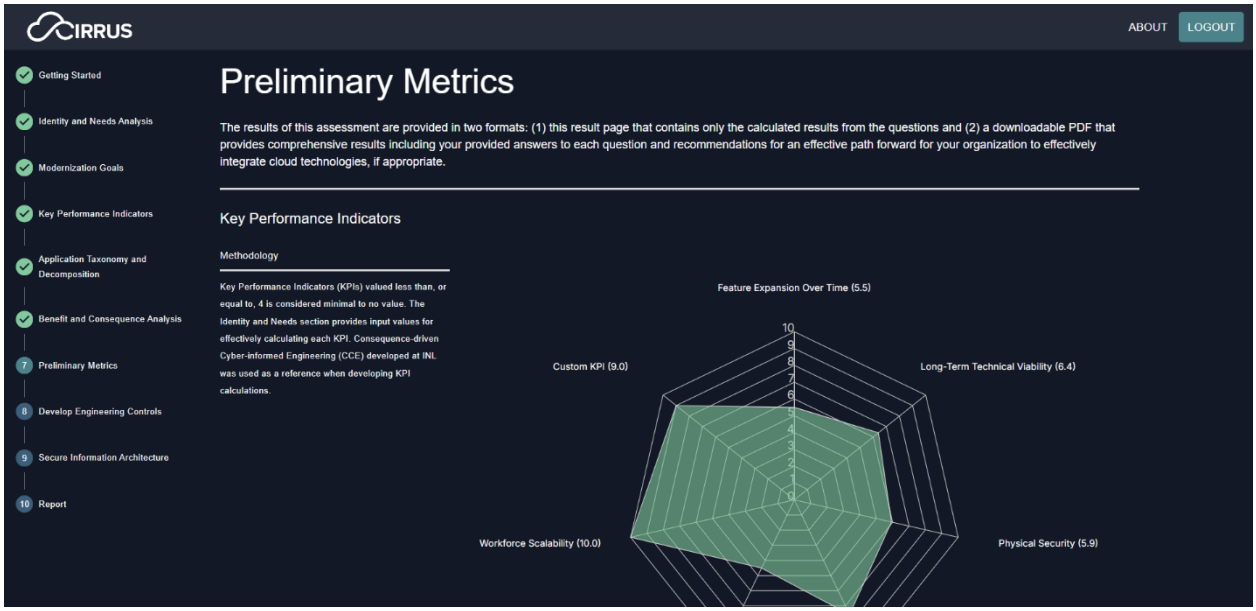
Table 1: Example consequence table and weighting.

Criteria	None	Low	Medium	High
Area/Load Impact	Inconsequential	Loss of failure to service firm load of less than XMW	Loss of failure to service firm load between X+1 and Y MW	Loss of failure to service firm load greater than Y + 1 MW
Duration	Inconsequential	Return of all service in less than 1 day (inability to serve firm load) or supply outage for less than one week	Return of all service 1 – 5 days (inability to serve firm load) (or) supply outage for 1 week – 1 month	Return of all service >5 days (inability to serve firm load) (or) supply outage >1 month
Safety	Inconsequential	Risk onsite	Definite safety risk offsite	Loss of life potential
Cost	Inconsequential	Significant but can recover	Multiple years to recover financially	Trigger of liquidity crisis/potential bankruptcy

Figure 4: Example of Cirrus' consequence matrices (DERMS).

Upon completion of Steps 1 and 2, a preliminary metrics snapshot (shown in Figure 5) is generated, outlining the risks and benefits of the application being considered. This result is recalculated for each application and produces a graph to fully understand and visualize techniques the organization may have to implement to mitigate the negative consequences associated with cloud technology implementation. Similarly to the consequence analysis, the benefits of the system are ranked and evaluated against the consequences. This insight is beneficial for planning resource allocation and developing mitigation strategies that would have the greatest impact.

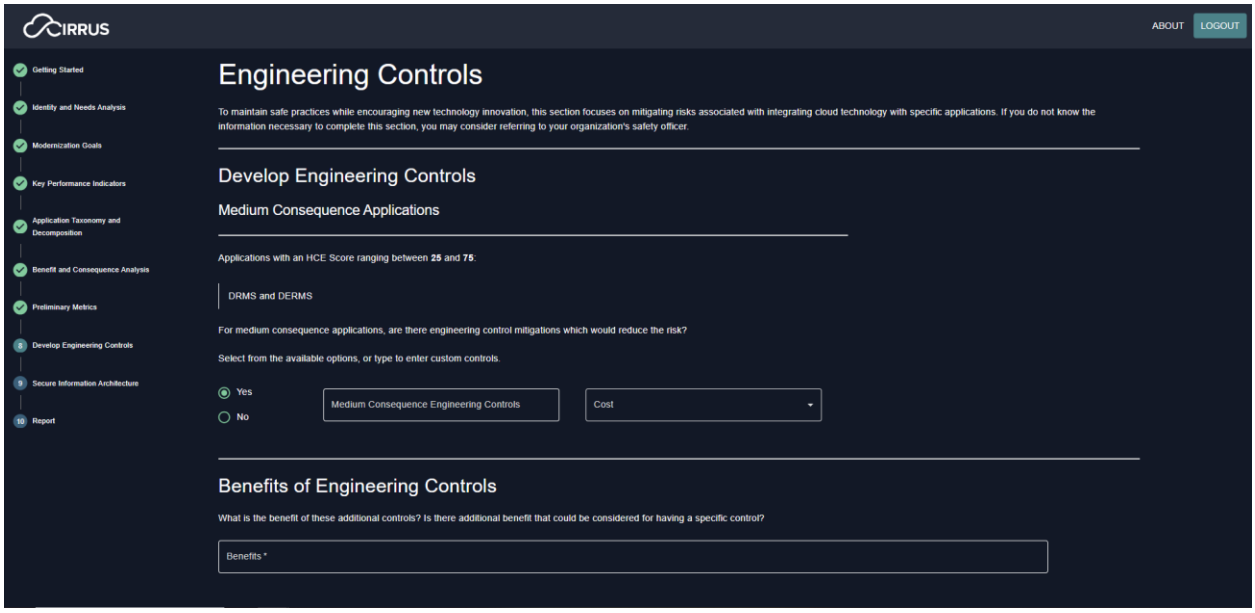
Figure 5: Cirrus' Preliminary Metrics page.



3. Develop Engineering Controls Around the Site

With risks identified and characterized by significance and probability (i.e., by the factors of likelihood and consequence), controls can be envisioned and implemented based on seriousness using the third evaluation construct. The initial questions involve understanding which controls could mitigate prioritized and highest-impact risks that the assessment taker has identified. During the "Develop Engineering Controls" assessment section (Shown in Figure 6 below), a series of engineering control suggestions are made for the application. Engineering control questions are asked in an open format to provide answer flexibility depending on who within the organization is completing the assessment. The benefit of using an open format for these questions is that it allows for a breadth of understanding, depending on the assessment taker's subject matter expertise.

Figure 6: Cirrus' Engineering Controls page.



The user is asked to add text input for other suggestions along with guidance on how to complete this, including which personnel of the team (e.g., engineering, cybersecurity, legal). For example, regardless of likelihood, the highest impact (i.e., loss of life) requires dynamic protections to be implemented. However, a second consideration is where the protections would be implemented. Is the control better positioned on local networks or in the cloud? To mitigate the highest impact risks associated with a cloud deployment of ADMS, particularly the catastrophic risk of loss of life (LoL), it is imperative to design and implement stringent controls within the cloud infrastructure. For instance, a dynamic protection strategy may involve the following aspects:

- **Real-Time Health Monitoring**: Implements continuous monitoring of system health to preemptively detect and address failure points.
- **Automated Shutdown Protocols**: Establishes automated safety protocols that can shut down compromised systems instantaneously to prevent accidents.
- **Hybrid Cloud-Local Controls**: Implements, especially in the case of Supervisory Control and Data Acquisition (SCADA) systems, a hybrid approach in which critical controls remain on-premises while non-critical data and processes use the cloud could offer a balance between functionality and safety.

A dynamic-protection approach is vital to address the high-impact consequences of cloud-deployed ADMS, specifically the risk of LoL. Controls within the cloud infrastructure can include real-time

monitoring and automated protective measures to prevent system failures. For SCADA systems, a hybrid local and cloud model could enhance resilience, ensuring critical operations continue even if cloud connectivity is compromised. It is crucial that controls are identified and integrated, even in vendor-designed ADMS, to safeguard against digital failures that could lead to human injury. The utility must work closely with the vendor to identify high-impact scenarios and ensure robust mitigation strategies are in place. When incorporating these controls, differentiation between what is included in the contractual product and service requirements and what is designed into the system is crucial. Some controls may need to be inherently built into the system architecture, while others can be specified as requirements from the CSP.

The feasibility of cloud deployment hinges on whether there are mitigations that make it a viable option without compromising safety. This involves a thorough cost-benefit analysis of the controls, such as investment in dedicated fiber, to ensure very low latency for protection systems run to the cloud. The benefits must be carefully considered, not only in terms of risk mitigation but also in the added value they provide, such as increased system uptime and improved response times. For the scenario in which an ADMS is designed by a vendor, the utility must collaborate closely with that vendor to pinpoint high-consequence risks. It is essential to ensure the digital and control failures that could lead to human injury are thoroughly understood and mitigated by safeguards that integrate robust controls that are both cost-effective and provide additional operational benefits.

4. Secure Information Architecture and Digital Asset Management Planning Evaluation and Consideration

System development relies on a life cycle assessment to ensure meticulous consideration of necessary materials and participating agents. This immense amount of information is created to define the system's purpose, design, elements and components, necessary skills required for operation, minimum viable product (MVP) performance, maintenance and operations procedures, and more. In the wrong hands, this information could aid an adversary in understanding system weaknesses, existing component vulnerabilities, and even human targets to aid in planning an attack. This information can unintentionally be released during procurement processes, often via public release, ensuring an open and fair competitive process. It can also be released in job listings, where specific technical criteria are used to find appropriate employment candidates, but may simultaneously reveal system features, and weaknesses and vulnerabilities to an adversary. The confidential information can additionally be shared in news articles or success stories about the system's entry into operations, where even a system photograph may release information valuable to an adversary.

During the "Secure Information Architecture" evaluation and the subsequent system-design process, the engineering team may use the Cirrus-provided prioritized list of consequences to identify what specific information should be withheld from public dissemination to avoid an undesired consequence. Administrative processes should be developed for protecting information, determining who can possess it, how to prevent inadvertent duplication and sharing, how to remove access, how to review and approve information release, and how to ensure team members understand the sensitivity of the information they have access to and how to protect it.

5. Simplification and Interdependency

An interdependency and CIE assessment for cloud deployment begins with an examination of the critical connections within the site. This Cirrus evaluation assesses how the communication systems intertwine with power operations and identifies any single point of failure (SPOF). The assessment evaluates the redundancy requirements and s failover protocols to ensure continuity of service. The goal of simplification requires the assessors to determine the dependencies of the highest-risk components on lower-risk elements such as Geographic Information System (GIS) access or data flows. Understanding the frequency and speed with which these interdependencies operate, along with the required data retention duration, is needed because longer storage leads to higher costs. Additionally, data throughput and storage costs must be assessed, especially if the system relies heavily on large datasets, to incorporate cost-effective measures in the deployment strategy. Assess the operational elements required for the application from other systems and their speed of integration. The following are items to consider:

- Examine interdependencies within the communication system and establish redundancy requirements.
- Evaluate data throughput and storage needs, considering the cost implications of interdependency, long-term and short-term storage, redundancy, and residency.
- Introduce simplification by identifying essential features for the cloud deployment, exploring the possibility of reducing features to mitigate risks, and determining the most crucial aspects within the device.
- Phase in features gradually with a heightened review of equipment capabilities over time, minimizing elements at risk for mission-critical functions in the initial deployment.

- Determine the minimum viable set of information and time duration required for the application to operate under conditions of temporary loss and for long-term benefits.
- Based on the insights gained from Step 4, provide data-handling guide references as a mandatory reading and evaluation step. Additionally, outline cloud-handling types and offer guidance on enhanced information protection considerations beyond the initial assessment and potential throughput concerns.

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

The digitization of U.S. energy infrastructure allows incredible benefits, such as providing speed and automation of operations that were not previously possible. However, digital assets and digitized functions have different weaknesses and frailty modes than their analog counterparts. Far beyond simple vulnerabilities to attack, these assets can function or be made to function in ways that their analog counterparts cannot, and consideration of these risks is important to ensure that the defensive measures for a system are cyber-informed. Digital asset awareness begins in design by considering that any digital device is, at its core, a general-purpose computer with specific command logic for its function layered on top. An attacker or, more rarely, a logic failure can subvert this logic and cause the device to ignore input, change values in command logic, or even execute commands or automated logic unexpectedly. The consequences considered earlier in the process can highlight specific impacts to mitigate in design, hopefully with controls that are not solely digital in nature.

Second, in operations, digital devices require different forms of maintenance, including patching and upgrades and the export of logs and commands stored on the system. To ensure that such systems are maintained in accordance with the function of our system, utilities must track the devices installed by hardware model, software version, patch version, location, last update, last export, system function, and so on. The system should also export logs and, if possible, retain them for forensic needs, and a "gold disk" configuration of the latest software and logic should be retained if needed. This ensures an understanding of where the systems are within their processes, what is occurring, how they are maintained, and any emerging risks identified as vulnerabilities. It also ensures that they can be restored or replaced if needed.

Even in the early design phases, engineers can establish the core security features and assumptions that every supplier should implement when bringing components or services into the system. These may include guidelines about required features in digital systems, limits on where such systems can be acquired, and how updates must be verified and signed. They may include practices for vendor behavior when providing onsite or remote maintenance. They may include requirements for sharing information about cybersecurity incidents, vulnerabilities, bills of materials, and vendors' development processes. Each of these controls contributes to the system's overall supply-chain security. These requirements should be discussed with those responsible for ensuring them, including procurement, cybersecurity, and system operators. For each control or feature, the team should consider how it will be verified, when and how often it can be verified, and who can perform the verification. These processes should be built into requirements for system development and operations, and verification should occur more than once for controls that could change or erode over time. The controls devised by the engineering team should be complementary to those leveraged by the organization's purchasing and cybersecurity processes, but because they are drawn from potentially catastrophic system consequences, they may well exceed the general due diligence performed by the organization.

7. Developing a Planned Resilience and Operations Model

The general operating mode of a system, with all functions available and working as expected, can be imagined; however, resilience requires that we imagine and plan for many different failure modes of a system, ideally including those linked to the set of prioritized undesired consequences created earlier. We must understand these failure modes, including how to operate through them, albeit at a lower level of performance or reliability. Ideally, a set of diminished operating modes can be created, which, though not ideal, can be built into expectations for well-understood modes of operation. These diminished operating modes should be integrated into the overall system operating modes, allowing for regular training, exercise, and assessment to ensure preparedness.

Certain functions within a system may not require quick communication or extensive critical function support. Understanding these aspects is essential to developing resilient operating modes. For instance, operations during a cyberattack may involve limited communication or reliance on critical functions, necessitating a strategic approach to ensure functionality even under constrained conditions. In such scenarios, it becomes pertinent to explore the potential transition of certain functions to a cloud-based or hybrid approach. By leveraging cloud capabilities, especially for noncritical functions, the system can enhance flexibility and adaptability during diminished operating modes.

Within each diminished operating mode, plans can be made for what would cause that mode, how that mode would function, and the changes to staff, systems, safety guidelines, performance, or other system conditions necessitated by the mode. Once this description is part of the overall set of system operating modes, it is reasonable to train, exercise, and assess performance in each of these diminished modes on a regular basis. These resilient diminished operating modes should include modes assumed because of a digital failure or cyberattack. For any critical system, diminished operating modes should include operations during an expected cyberattack involving one or more of those systems, operating when the team is uncertain of the validity of the data emerging from the system, where critical automation logic is not dependable, or where core network connections or support services are not available.

It is likely that exercising these modes will require the operations team to pair with cybersecurity counterparts and understand the roles and responsibilities each team member will perform. These operating modes may also require that the team consider altering the system design to allow limited manual operation options when digital systems are not operating or trusted. Considerations for PR should also include how untrusted systems can be restored to full function within the system context, including what operational steps will be required to ensure future trust or whether that is possible given the function of the system or component.

8. Discussion on Clouds and Cybersecurity Culture

The integration of cloud computing into an organization’s infrastructure intersects significantly with cybersecurity culture. Shared beliefs, perspectives, and values regarding cybersecurity dictate how a group prioritizes investments and actions to enhance its realization.

Engineering design teams, mindful of the ramifications of digital failure or cyberattacks on systems under development, hold a fundamental responsibility to educate all stakeholders on cybersecurity. This includes those accountable, responsible, consulted, or informed about the system, illustrating how each stakeholder’s role can positively or negatively impact overall system security. Developing a data flow diagram for visual representation of system connectivity provides team members with a holistic understanding of upstream and downstream impacts.

Equally crucial is providing comprehensive cybersecurity training to employees, covering technical aspects while instilling a cybersecurity mindset. Regular training sessions ensure employees are ahead of the latest threats and best practices, bolstering the organization's overall cybersecurity resilience. This entails managing security measures, ensuring regulatory compliance, and continuously monitoring the cloud environment. Close collaboration with the cybersecurity team is important to align strategies and fortify cloud infrastructure resilience. Eliminating workarounds and thoroughly scrutinizing modifications due to vendor engagements are imperative. This necessitates assessing their impact on organizational cybersecurity measures and adjusting strategies accordingly. Vendor collaboration should seamlessly adhere to organizational security standards, ensuring any alterations enhance rather than compromise cybersecurity posture.

Incorporating CIE and All Hazards Analysis (AHA) is vital for utilities contemplating migration to cloud services. This approach involves evaluating potential impacts from various threats, spanning cyberattacks to natural disasters, along with operational efficiencies to maintain reasonable costs and consumer energy prices. By assessing the consequences of potential hazards, utilities can prioritize critical asset and function protection. This entails identifying vulnerabilities, gauging scenario likelihoods, and discerning operational and financial implications. Such a comprehensive risk assessment informs the development of security measures and incident response plans, ensuring utilities are adequately prepared to safeguard and manage cloud network environments.

Figure 7 depicts the level of responsibility retained by the system owner, depending on the chosen cloud architecture. There is a common misconception that migrating systems to cloud providers results in the transfer of all security, management, and risk responsibilities to the provider. However, it is crucial to recognize that, particularly in sectors like Cloud of Things (CoT) or Industrial Control Systems (ICS), some level of responsibility will persist with the utility for security updates and maintenance, contingent upon the implemented cloud model.

Figure 7: Cloud architecture model.

After conducting a thorough risk assessment with Cirrus, all outputs described above are compiled in a PDF based (shown in Appendix) on the information provided. These outputs aid in determining the most suitable cloud service model (SaaS, IaaS, PaaS) for each entity's initiative and business needs. Determination is based on resource requirements, budget constraints, and available personnel to support the cloud initiative.

PROTECT

The integration of cloud computing into OT (Operational Technology) infrastructure is crucial for enhancing security and resilience. Historically, OT systems operated in isolated networks, which provided a natural barrier against cyber threats. However, with the increasing demand for optimization, visualization, and integration with IT networks, these systems are now more exposed to potential cyberattacks. Cloud computing offers advanced security measures such as encrypted data storage and transmission, continuous monitoring, and automated threat detection. These features collectively ensure that OT systems are protected against modern cyber threats while maintaining operational efficiency and compliance with regulatory standards. By leveraging cloud solutions, organizations can create robust, self-healing, and resilient networks that safeguard critical infrastructure from both digital and physical threats.

Build Secure and Resilient Networks

Stakeholders and vendors operating legacy on-premise OT utility power systems were able to get by with lax cybersecurity controls in the past due to the nature and isolation of networks that contained OT equipment and systems that were built on an island or isolated from external connectivity. In the last decade and a half, there has been an ever-growing demand for optimization and visualization into these networks to get metrics and historical data to predict load, as well as increase efficiency. The added renewable energy market also adds complexity into DER-based operations to account for load demands requiring additional balancing of operations based on loads that dynamically change grid operations and visibility.

The increased network connectivity to these systems has created many challenges in the realm of securing data and networks in this infrastructure, along with adding complexity of additional stakeholders managing these systems. Evaluation of these legacy networks and security controls within these systems will need to be considered when connecting to a cloud-based architecture to ensure that physical-based systems are not a threat vector for newly cloud-created systems. The following foundational items need to be considered:

1. Networking is the foundational piece of IT and OT networks due to the requirements of applications and business tools. Cloud-based connectivity will need to be as, if not, more resilient and fault tolerant than traditional networking for entities managing grid operations and control centers. Data going to the cloud will be required to be not only resilient, but self-healing for cloud migrations. Cloud-based networks not only will it need to resilient, but also require cybersecurity encryption best practices will need to be followed.
2. Encryption is a key part of any cloud security strategy. Not only should organizations encrypt any data in a cloud storage service, but they should also ensure that data is encrypted during transit — This is when it will be most vulnerable to attacks. Encryption options will be available from your cloud provider, work to ensure the options they provide meet your overarching security policy and encryption standards for your organization.
3. Some cloud computing providers offer encryption and key management services. Some third-party cloud and traditional software companies offer encryption options as well. The recommendations of finding an encryption product that works seamlessly with existing work

processes is recommended, eliminating the need for end users to take any extra actions to comply with company and regulated encryption policies.

4. Encryption for networks services should be transparent to users of the system but does create additional overhead to operate correctly by adding layers into the network TCP\IP stack. The details of this are beyond the scope of this paper, but these considerations need to be assessed and taken into consideration as sizing for connectivity selected for bandwidth requirements to the cloud hosting provider from the on-premise locations.
5. Encryption alone will not be enough to protect data networks. Micro-segmentation and evaluation of what data and access are being aggregated across networks and applications needs to be fully assessed in complex cloud networks to ensure that virtual and containerized networks adhere to the same best practices as physical networks and isolation and protection. Containerized applications and access via micro-services need to be accounted for and rules applied to limit access.

Select a Cloud Service Provider (CSP)

In addition to clarifying shared responsibilities, organizations should inquire about the security measures and processes implemented by cloud vendors. Assuming leading vendors have security covered can be misleading, as security approaches can vary significantly among vendors. Conducting due diligence involves ensuring that the security requirements of the prospective cloud provider align with the organization's security posture and assessing whether they meet the needs of the organization, or if adjustments can be made to fulfill these requirements in accordance with the overarching security policy.

To comprehend the organizational structure and business practices of a specific cloud provider, it is essential to evaluate alignment with business objectives. This document outlines a series of questions that organizations can pose to cloud providers to determine suitability for utility electric projects. These questions span a wide range of topics, including:

- Is there a security framework that the cloud provider adheres to?
- Where do the provider’s servers reside geographically? Global or US/EU only?
- What is the provider’s protocol for suspected security incidents?
- What is the provider’s disaster recovery plan?
- What measures does the provider have in place to protect various access components?
- What level of technical support is the provider willing to provide and cost associated?
- What are the results of the provider’s most recent penetration tests?
- Does the provider encrypt data while in transit and at rest?
- Which roles or individuals from the provider have access to the data stored in the cloud?
- What authentication methods does the provider support?
- What compliance requirements does the provider support?
- What type of cloud application security brokers do they support?
- Do containerized applications span multiple data centers and countries requiring more resources?

Develop and Implement Cloud Security Policies

All organizations should establish written guidelines outlining the permissible usage of cloud services, the approved methods of utilization, and the types of data eligible for cloud storage. They also need to lay out the specific security technologies that employees and vendors must use to protect infrastructure, data, and applications in the cloud. The impetus to having a long term secure and securely architected system starts with having a policy that ensures business conducted in the cloud is done via policy.

The drive towards establishing a secure and well-architected system for the long term commences with implementing policies that dictate cloud-related business practices.[4] Rushing to adopt cloud solutions without tailor-made policies often results in attempts to integrate these implementations into conventional IT-based policies, leading to operational challenges and unforeseen security issues stemming from cloud complexities.

Cloud Security Policy

To illustrate effective cloud security practices, Table 2 demonstrates an example of a written cloud security policy:

Table 2: Security policies for reference to create effective cloud security practices.

Section	Details
1. Identify the Scope	• This policy applies to all <company name> employees, contractors, and third-party users utilizing cloud computing services in their duties.
2. List Ownership and Responsibilities	• Chief Information Security Officer (CISO) oversees and implements the policy. • IT department handles technical implementation and enforcement. • All employees and users must comply with the policy.
3. Define Secure Usage of Cloud Computing Service	• IT/OT department maintains an up-to-date inventory of cloud services. • Regular reviews and updates of the inventory. • CISO/Asset owner maintains a list of approved cloud services. • Only approved services may be used. • Unauthorized cloud services are prohibited. • Report unauthorized usage promptly.
4. Determine the Areas for Risk Assessment	• CISO/Compliance conducts periodic risk assessments of cloud services. • Evaluates risks related to data privacy, compliance, and business continuity.
5. Implement Security Controls	• IT/OT department or 3rd party integrator implements security controls like encryption, access controls, and authentication. • Regular review and update of security controls based on risk assessments and/or yearly audits.

6. Develop Security Incident Recovery Plan	• CISO/Stake Holder develops and maintains a cloud incident response plan. • IT/OT department notifies CISO and follows response procedures for incidents. • Ensure data backups are available and tested yearly
7. Raise Awareness through Training	• CISO and IT department provide ongoing cloud security awareness training. • Employees and users must participate and promote security culture. • Enhanced permissions users require additional cybersecurity training.
8. Enforcement/Review	• Violations may lead to disciplinary action or termination for employees and contractors. • Third-party users may face contractual penalties. • Compliance with audit and reporting metrics required by compliance bodies.
9. Related Documents	• CISO and IT/OT department maintain and refer to: • Cloud computing service agreements. • Data classification and handling policy. • Incident response plan. • Adhere to training materials and related documents.
10. Review and Revision	• Policy will be reviewed and updated periodically. • Users are encouraged to provide feedback for improvement.

Identity and Access Management and Control Plan

Unauthorized access is a major concern with cloud security. Organizations looking to move Utility Infrastructure and DER-based systems, along with 3rd party applications into cloud providers, should consider building comprehensive identity and access management (IAM) systems based on the following principles to minimize risk:

1. Organizations should be capable of designing and enforcing access controls rooted in the principles of least privilege and zero trust. This involves limiting user access to only essential tasks and treating all access requests with vigilance. The process of adding and modifying user permissions and accounts within the system should be complemented by change management (CM), ensuring that all actions are documented. Implementing privileged access management (PAM) accounts can enhance security for the most sensitive accounts by providing oversight and control.
2. Implement multi-factor authentication (MFA) to increase security. If adversaries obtain credentials like usernames and passwords, MFA creates an additional layer of security by demanding additional verification, such as biometric scans, rotating pins, or SMS codes.
3. Combine and implement IAM policies that offer permissions that can be tied to role-based access control (RBAC)**.** RBAC is based on the least privileged model, this help guarantees that users' access is provided based on their unique positions within the company, decreasing the possibility

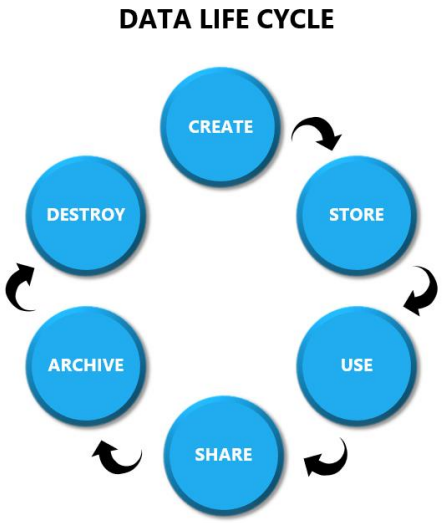
of unwanted access. When users leave the company accounts with higher elevated privilege should be changed if not paired with multifactor authentication (MFA).

4. The use of shared accounts should be avoided when implementing systems and software solutions in cloud. Most ICS systems require system accounts for operation between systems and applications, as well as connections into Database Management System (DBMS). These accounts should be monitored for abnormal usage and notifications created when non system events occur. These accounts are often compromised, and no monitoring is done against system accounts that have elevated privileges.
5. Consider IAM solutions that can operate across private data centers and cloud deployments**.** This streamlines end-user authentication and allows for uniform policy enforcement across all ICS/OT environments.

Security Strategies for Data Storage

The methodology for cloud networks in the data storage arena will be a key focus of the cybersecurity effort. There will be a need to move historical data that exists in the current grid platforms to cloud-based storage and have immutable storage capabilities, along with supporting real-time operations and data creation by having the complete dataset for operations centrally located. Figure 8 shows the general principles of the cloud data life cycle for grid or OT operations, which are also discussed below.[5]

Figure 8: General principles of the cloud data life cycle for grid/OT operations.



1. Create

Unlike traditional on-premise data or IT cloud data creation, data from control systems may or may not originate in the cloud, given that many of the Utilities systems will be physically located at a particular physical remote site that could be geographically dispersed. Data from these remote physical sites and systems will need to be encrypted before being transmitted to the cloud, to then be utilized by not only the entity that is operating the grid but also available to other 3rd party system integrators that may need to remediate operational issues based on the metrics being collected. A comprehensive data classification system should be in place prior to data creation and storage. All data types will need to be identified prior to creation and secure data to the appropriate level of classification.

2. Store

Data generated from utility control systems and supporting operations will require data storage. Communications requiring remote storage from a physical site to cloud site will need to be encrypted in transit. Even though some data may also be stored locally, the best practice is to have communications and stored data encrypted as well. Remote and local storage of data will have classification and appropriate controls applied; this will make long-term data retention and audits easier to complete based on having a complete view of what data types exist and retention periods defined.

3. Use

One of the most complex items of cloud data is the multiple access methods that. Almost all data will be accessed by remote connections, or networked access, as well as access via application programming interfaces (API). These all require secure connections to prevent access and or manipulation of data in transit. Given the various number of access methods available and the wide range of users and organizations that could require access to data sets that pertain to grid operations, a very detailed comprehensive data security access plan will need to be created, and the security controls of each one will be carefully architected. The periods of data access and limitations should be defined in an acceptable use policy, and durations of access should be enforced. RBAC policies should also be strictly enforced to control and mitigate access to only the data needing to be accessed by each user and or group that needs it.

4. Sharing

Various organizations will require access to data contained in grid-based implementations to operate and maintain grid operations or supporting systems that are storing data in the cloud. The greater the access footprint and shared access to data in the cloud, the greater the risk to operations and doing business. Information rights management (IRM) solutions combined with RBAC solutions will need to be implemented to fully secure the data being accessed and have a clear understanding of all the users and entities that have data access over time. These solutions will need to be combined with data loss prevention (DLP) for a complete end-to-end solution and create accountability for all access and storage.

5. Archive

All data stored in the cloud needs to employ some form of cryptographic control. This will be defined by the scope of the overarching security policy and classification of the data type. Most cloud providers offer long-term, ephemeral, and raw storage. They also evaluate what each provider offers and verify that your business objectives can be met.

Below are key items to consider when evaluating your cloud data archive:

Location:

- Where is the data being stored by the cloud provider?
- Are Multiple providers involved?
- What environmental factors exist that could impact risk.
- Climate?
- Natural disasters?
- What Jurisdictional items may impact storage?

- Local or National Laws or regulation?
- What data access impacts exist if forced to operate during contingency planned events.
- Is Backup data far enough away from production data in the event moving to your disaster recover (DR) plan?
- Is data replicated in multiple locations and multiple clouds?

Format:

- Do you know what types of format or media are stored during production?
- Do you know what media type and location data is stored on when offline and replicated?
- Is any media kept or stored in portable devices that need extra security controls against theft
- What is the length of time you are required to keep data, and do you have enough storage contractually to meet your obligations

Procedure:

- How is cloud data recovered, and what process exists to restore data?
- Who has authorization on the cloud side for your data recovery?
- Who on utility/vendor side has access to request recovery operations?
- What is the frequency of backup and types of backups and restore operations being performed to very that restoration can occur?

6. Destroy

At some delineated point in time, data retained in the cloud will exceed its value of being stored versus the cost of having it accessible, backed up, and stored offline. The cost of maintaining storage and budget spending on the required resources to protect it will exceed the point of feasibility. The need for data destruction may be based on its usage and retention requirements, as well as any regulatory requirements for retention. Cloud providers often have the capability to provide full-service data management plans for managing the full data life cycle. Consult with your cloud provider to evaluate and validate data retention policies being enforced for the different data types listed below:

- File Based Storage
- Block Based Storage
- Object-Based Storage
- Database Production and replication Dataset.
- Security Strategies and Encryption were used for each data storage type.
- Validate that any Encryption Keys created have been destroyed and are not recoverable.

DETECT

Cloud computing can significantly enhance the ability of Operational Technology (OT) environments to detect operational and security issues by leveraging advanced logging, monitoring, and centralized management tools. By enabling comprehensive logging in cloud services and implementing a Security Information and Event Management (SIEM) system, organizations can monitor user and system activities in real-time, detect unauthorized modifications, and track changes that could lead to vulnerabilities. This

proactive approach not only helps in identifying misconfigurations and people with excessive access rights but also in taking preventive measures to reduce security risks such as unauthorized access, data breaches, and lateral movement by malicious actors. The integration of cloud-based tools like AWS CloudTrail provides a clear record of actions taken, facilitating quick remediation and minimizing the risk footprint, thereby maintaining the integrity and security of OT systems.

Enable and Monitor Security Logs

Logging and Monitoring in the cloud is one of the most effective cloud security options available today. Organizations should enable logging in their cloud services and take it a step further by creating and making available an SIEM system for centralized monitoring and response. Logging helps system administrators and security teams monitor user and system activity to detect unapproved modifications, logins, and activity, a process that would be impossible to accomplish manually. In the event that an attacker gains access and makes changes to systems, the collection of logs offers a clear record of the actions taken, along with information about the time and applications used to make unapproved modifications. An SIEM tool will allow for quick remediation to limit damage and data compromise of the underlying systems and limit the risk footprint by having various notification types alert personnel of items needing remediation. In AWS, for example, CloudTrail log files can be imported into an AWS CloudTrail Lake or third-party SIEM tool for analysis, which will typically be priced by volume. Tools like CloudTrail are just an example of one of the many tools in the SIEM market that can provide part of a layered security model.[6]

Log Misconfigurations

Effective logging is also important for dealing with misconfigurations because it enables tracking of changes that can lead to vulnerabilities and allows for preventive steps. It also assists in detecting people with excessive access rights, allowing for changes to be made to reduce possible operational failures. It is essential not just to log misconfiguration data but also to take proactive steps to reduce misconfigurations in storage buckets, APIs, connections, open ports, permissions, encryption, and more. Some cloud services provide extensive rights by default, sometimes even to external users, posing serious security vulnerabilities if not restricted properly; default public settings for AWS S3 buckets is one such example. Misconfigurations provide chances for malicious actors to:

- Steal from cloud buckets.
- Move laterally through the storage infrastructure if they obtain the right credentials.
- Move laterally through the container network if not properly configured with the least privilege.

Improper account permissions might allow attackers who steal credentials to gain administrator access, resulting in additional data breaches and possibly cloud-wide attacks. Although the work is time-consuming, it is critical for your company's IT, storage, or security teams to:

- Personally configure each bucket or group of buckets.
- Collaborate with development teams to ensure that web cloud address setups are correct.
- Ensure that the default access permissions are never used.
- Determine the user access levels that are required (view-only or editing rights) and configure each bucket accordingly.

Tools like cloud SIEMs, cloud workload protection platform (CWPP), cloud security posture management (CSPM) and cloud-native application protection platform (CNAPP) can help. Having a full understanding of tools available by your security provider to help troubleshoot and identify misconfigured equipment will be key in leveraging the next generation cloud tools and analytics.

Audit and Compliance

Deploying the controls outlined in this document will streamline reporting procedures for audits and compliance within the cloud environment. It will expedite mandatory regulatory audits by pre-compiling metrics for immediate consumption. The capability to consolidate data from various vendors and supporting systems into cloud-native formats will establish a seamless reporting framework. The subsequent activities will establish a foundational framework for auditing and reporting. Whether an organization partners with an outside security firm or keeps security functions in-house, it's recommended to conduct the following security practices on a defined schedule based on the overall cybersecurity plan implanted for ICS/OT systems residing or connected to the cloud:

Penetration Tests

- ✓ Examine the reliability of present cloud security solutions.
- ✓ Identify vulnerabilities that might put data and applications at risk.
- ✓ Identify vulnerabilities that put network and servers at risk.

Vulnerability Scans

- ✓ Use cloud vulnerability scanners to detect misconfigurations and other flaws.
- ✓ Enhance the security posture of the cloud environment.

Regular Security Audits

- ✓ Assess all security vendors and controls to determine their capabilities.
- ✓ Make sure vendors and users follow agreed-upon security terms and standards.
- ✓ Validate security policies are being followed and enforced.

Access Log Audits

- ✓ Ensure that only authorized individuals have access to sensitive data and cloud apps.
- ✓ Improve access control and data security measures.
- ✓ Verify all sources configured for log reporting are working as designed.

Tabletops and Incidence Response

The North American Electric Reliability Corporation (NERC) works with entities to conduct tabletop exercises for grid operations on a cadence. Every two years, the Electric Information Sharing and Analysis Center (E-ISAC), GridEx gives E-ISAC member and partner organizations a forum in which they can practice how they would respond to and recover from coordinated cyber and physical security threats and incidents. It is the largest grid security exercise in North America.[7] The scope of these tabletops is prepared with a set scenario that the E-ISAC establishes. A technical approach similar to this will need to be taken with cloud-hosted solutions that support Grid operations as electric providers start to segway into leveraging the cloud and moving electric control into an environment that is not fully physical and combines elements of virtual and physical. The combination of traditional tabletop and cloud-based tabletops will need to be leveraged, and scenarios created to fully understand the risk present. Below are tabletop and incidence response components to consider:

- Cloud-based simulations can also be created to simulate attacks to see what cyber-physical items can be exposed to help mitigate risk.
- IR solutions can be created based on the new cyber-OT cloud to physical elements present.

- Updated Operational documents will be created from scenario-based outcomes.
- Expanded training and education may be required for all OT\IT supporting grid operations.

RESPOND AND RECOVER

Cloud computing significantly enhances the operational technology (OT) sector's ability to respond to and recover from cyber and physical threats by providing scalable, flexible, and integrated solutions. By leveraging cloud-based simulations and Incident Response (IR) solutions, organizations can create realistic scenarios to identify vulnerabilities and devise mitigation strategies. Cloud platforms enable real-time data analysis and visualization through tools like Malcolm and Splunk, allowing for swift detection and response to security incidents. Furthermore, the integration of cloud services with traditional OT systems facilitates expanded training and education, ensuring that all personnel supporting grid operations are well-prepared to handle complex cyber-physical security challenges.

Cloud Tools and Applications

For broader cloud security assessments, organizations typically complement endpoint protection with dedicated cloud security tools and frameworks. Organizations are beginning to recognize the importance of fortifying their digital assets beyond traditional endpoint protection. For a holistic approach to cloud security assessments, dedicated cloud security tools and frameworks play a crucial role in ensuring the integrity, confidentiality, and availability of data and services. These specialized tools are designed to address the unique challenges posed by the cloud environment, ranging from identity and access management to encryption, network security, and compliance monitoring.

Case Study: Building Cirrus as a Secure Cloud Tool

Cirrus itself is a software asset hosted on cloud infrastructure and implements industry leading best practices in cybersecurity policy to protect itself and its users. These practices broadly emulate the ISO/IEC 27000[8] family of standards, and INL also inherits DOE information technology governance strategies. The result is that Cirrus obeys industry leading development, security, and operations (DevSecOps[9]), and change management processes.

Engineers involved in the development and deployment of cloud applications like Cirrus run a gauntlet, fortifying their application’s ability to resist penetration tests, auditing their application’s third-party dependencies, and constructing resilient production environments. Further, cybersecurity teams manage a suite of vulnerability assessment tools that notify application owners of any newly discovered vulnerabilities harbored by the application after its release, indicating in real-time whether a patch is needed. INL change management experts also require extensive written documentation about the application’s ability to handle CUI or PII data types, in addition to documentation demonstrating the architectural patterns in use for data transfer, and storage.

Software engineers and their cybersecurity counterparts work together in a dual-control or split-knowledge pattern to develop pipelines which build software artifacts and deploy them into their respective cloud environments.[10] Software engineers retain the liberty to make changes to the source code, and build resulting artifacts, but every release of additional code or infrastructure fall under the same change management practices.

Cirrus is hosted on government cloud infrastructure, and as such adapts National Institute of Science and Technology (NIST) guidance found in its Cybersecurity Framework (CSF).[11] This framework guides the development of a bespoke cyber-secure IT posture involving patterns like the hub-and-spoke architecture, dual-control or split-knowledge responsibilities, and automated vulnerability scanning.

Cirrus developers resultingly obey the same kind of standards that are otherwise expected of Cirrus users exploring the feasibility of managing their software applications in cloud environments.

Vulnerability Detection

1. Malcolm

Malcolm is an open-source suite built for advanced network traffic analysis, offering enhanced capabilities and ease of deployment. It supports network data inputs such as full packet capture (PCAP) files and Zeek logs, which can either be uploaded via a web interface or captured live and forwarded for processing. Once ingested, the data is automatically normalized, enriched, and correlated for further analysis. Malcolm operates as a cluster of Docker containers, providing network communication visibility through two user-friendly interfaces: OpenSearch Dashboard for flexible data visualization and Arkime for in-depth session tracking.[12]

2. Splunk

Splunk[13] is a platform designed to help organizations process and analyze machine-generated data. Its features for search, analysis, visualization, and monitoring support the management and extraction of information from large, diverse datasets. Splunk provides free, self-paced training courses and can scale resources according to data volume, using a pay-as-you-go model for cost efficiency. The platform's cloud accessibility allows teams to collaborate across different locations, while high availability and disaster recovery options enhance operational reliability. Additionally, Splunk integrates with various cloud services and data sources to maximize the use of cloud infrastructure.

3. Snort

Snort[14] is an open-source intrusion detection and prevention system designed to improve network security, including in cloud environments. Its primary function is real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort can operate as both a network intrusion detection system and a network intrusion prevention system. It monitors network traffic, analyzing packets for potential signs of malicious activity or predefined patterns that may indicate a security threat, such as known attack signatures or unusual behavior. In cloud environments, Snort can be deployed to help protect virtualized infrastructure by inspecting network traffic and identifying potential risks, which is important in distributed environments where data and applications span multiple servers and locations.

4. Nessus

Nessus[15] is a vulnerability assessment tool designed to identify security vulnerabilities, misconfigurations, and weaknesses within a network. Nessus scans systems and networks for known vulnerabilities and provides detailed risk analysis. It uses a database of thousands of plugins covering a wide range of vulnerabilities to ensure a thorough examination of the target environment.

Nessus generates reports that prioritize vulnerabilities based on severity. With the ability to integrate with various cloud platforms, Nessus provides options for organizations seeking to enhance their cloud

security defenses. Its user interface and regularly updated vulnerability database assist in maintaining continuous vulnerability management.

All Hazards Analysis (AHA)

The All Hazards Analysis (AHA) framework, developed by Idaho National Laboratory (INL), is a tool designed for analyzing critical infrastructure dependencies and risks.[16] It enables decision-makers and emergency managers to gain a comprehensive understanding of interconnected infrastructure systems by identifying dependencies and associated risks. AHA utilizes a function-based approach to model infrastructure as nodes and links, continuously updating with new information and changes in network structure for detailed sector and consequence analysis.

The tool provides a baseline dataset from open-source and user-provided data, secured and accessible only to authorized users. It features both geospatial and graph visualization capabilities, allowing data to be viewed through linked Map Views and Dependency Graphs. AHA's user-friendly and customizable interface enhances its usability and integrating it with cloud environments can further improve its data collection, storage, and real-time analysis, making it a robust solution for managing and understanding critical infrastructure.

Open-Source Threat Intelligence

1. Shodan

Shodan[17] is a search engine that scans and indexes devices connected to the internet, offering users visibility into online assets. Unlike traditional search engines that focus on website content, Shodan collects data about various devices, including servers, routers, webcams, and other internet-connected devices. Users can search for specific devices, services, or vulnerabilities.

From a security standpoint, Shodan can be used by cyber professionals and ethical hackers to assess the exposure of devices and identify potential security risks. It allows for the discovery of misconfigured or vulnerable devices that may be at risk of unauthorized access.

2. Maltego

Maltego[18] is an open-source tool designed for conducting open-source reconnaissance on organizations. It combines publicly available information to create a visual representation of the connections a business has with other entities. Maltego can also display documentation related to a business, which helps organizations understand what information may be publicly accessible and identify any sensitive data that might require attention. By linking analysis and data mining, Maltego provides a comprehensive view of the data collected.

Endpoint Threat Detection

1. CrowdStrike Falcon

CrowdStrike Falcon[19] focuses on endpoint security in cloud and on-premises environments. Crowdstrike Falcon utilizes cloud-based architecture and artificial intelligence to offer threat detection and response capabilities. Organizations that implement CrowdStrike can gain real-time visibility into endpoint activities, enable rapid threat detection, and enhance their ability to respond to security incidents.

Additional Considerations

1. Cirrus

As referenced in Section 1, the Cirrus framework is designed for organizations considering either a transition or an early application of the cloud. This framework does not provide a definitive yes or no; rather, it offers strategic guidance on how to prepare for, deploy, or improve a cloud solution responsibly. The approach integrates INL's CIE framework[20], which was a core consideration when building the tool. The user-provided inputs form the basis for developing a tailored cloud strategy. The final report generated by Cirrus, detailed in Appendix A, encapsulates crucial elements essential for cloud implementation.

2. CISA KEV Catalog

The Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) Catalog[21] is a resource for organizations addressing cybersecurity threats. This catalog, curated by CISA, provides a comprehensive list of vulnerabilities that have been exploited in real-world situations.

Organizations are encouraged to prioritize the remediation of vulnerabilities identified in the KEV Catalog to mitigate the risk of compromise by known threat actors. While federal civilian executive branch agencies are required to address these vulnerabilities under Binding Operational Directive (BOD) 22-01, CISA indicates that this guidance applies to all organizations, including state, local, tribal, and territorial governments, as well as private industry entities.[22]

3. CISA's Cybersecurity Evaluation Tool

The Cybersecurity Evaluation Tool (CSET)[23] is designed for the systematic evaluation of an organization's security posture. It provides a structured approach, guiding asset owners and operators through step-by-step processes to assess both industrial control systems and IT network security practices. CSET enables users to align their cybersecurity measures with established government and industry standards. Additionally, CSET can conduct ransomware readiness assessments.

4. FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP)[24] is a U.S. government-wide program that standardizes the security assessment, authorization, and continuous monitoring of cloud products and services. This program establishes unified security standards based on National Institute of Standards and Technology (NIST) guidelines, categorizes cloud services into three impact levels, and employs a collaborative authorization process that involves a thorough evaluation of security controls.

It features a centralized marketplace that showcases pre-authorized cloud solutions, facilitating the procurement process for federal agencies. The involvement of third-party assessment organizations (3PAOs) adds an independent component to the security assessment process, contributing to the overall improvement of cybersecurity practices within the federal government.[25]

5. NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF)[26] offers a flexible set of guidelines and best practices for managing and minimizing cybersecurity risk. When working with operational technology (OT) systems in cloud environments, it is important to consider both the NIST CSF and NIST SP 800-82[27] to address the differing requirements of OT compared to cloud IT.

6. Cyber-Informed Engineering Implementation Guide

CIE provides a framework to embed engineering controls and cybersecurity considerations at the foundational levels of design and operation. The CIE implementation guide deep dives into twelve CIE principles.[28] These principles assist stakeholders in integrating defense mechanisms against cyber threats starting from the initial design phase. The following CIE principles should be considered in each phase of a system's engineering life cycle:

4. Consequence-Focused Design
5. Engineered Controls
6. Secure Information Architecture
7. Design Simplification
8. Layered Defenses
9. Active Defense
10. Interdependency Evaluation
11. Digital Asset Awareness
12. Cyber-Secure Supply Chain Control
13. Planned Resilience
14. Engineering Information Control
15. Organizational Culture

SUMMARY AND CONCLUSIONS

There is no one size that fits all when applying cybersecurity controls and securing utility power systems that make DERs, Microgrids, and complex integrated vendor systems, let alone a single solution that can be engineered in the realm of securing OT/ICS systems and applied uniformly. Each utility vendor and stakeholder implementation combined with the unique nature cloud vendors makes it impossible to have one model that can secure all these systems. The objective of this paper was to take the engineered and implemented systems and have an outline of cyber controls applied to the various technical disciplines that make up complex utility systems. A more specific and prescribed posture for the technology system and manufacturers' requirements will be needed for access, monitoring and storage.

The security controls selected will need to meet the business needs of the project for a secure implementation in the cloud or hybrid cloud model. The combination of these technologies and cybersecurity controls will be combined to create a more resilient and secure energy-based system for next generation power management that allows easier integration as new technologies and advancements emerge and can be combined with legacy power systems in a secure manner.

There will be elements in each of the disciplines listed in this document used to build a comprehensive and complete cybersecurity posture paired with existing cybersecurity frameworks that seek to operate utility-based systems in the cloud. This guide to cybersecurity controls is to be used in tandem with the Cirrus framework, aiding organizations as they start down the path to migration into cloud hosted systems to further make managing, securing and reporting on cloud utility-based systems more manageable and secure.

ADDITIONAL ACKNOWLEDGEMENTS

Additional acknowledgements for Cirrus tool development are extended to Abby Neumann, Adam Altaii, Hannah Warren, Jake Swinford, Maria Lopez-Delgado, Samantha Thueson, and Tad Decker for their contributions to the development of the Cirrus tool.

REFERENCES

[1] Stewart, E., J. Morgan, and R. Stolworthy. 2024. "Use Case-Informed Framework for Utility Cloud Migration." *Idaho National Laboratory.* https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_112007.pdf.

[2] Netsapiens. n.d. *Geo-Redundancy.* https://www.netsapiens.com/geo-redundancy/.

[3] Liu, Y., and E. Stewart. 2021. "Distribution System Planning and Operation to Facilitate High Penetration Levels of Distributed Solar PV." *U.S. Department of Energy.* May. https://www.energy.gov/sites/default/files/2021-05/Distribution%20Liu%2.

[4] eSecurity Planet. 2023. *Cloud Security Best Practices: Enable and Monitor Security Logs.* April 21. https://www.esecurityplanet.com/cloud/cloud-security-best-practices/#enable-and-monitor-security-logs.

[5] ISC2. 2022. *CCSP Certified Cloud Security Professional Official Study Guide (2nd ed.).* https://www.isc2.org/certifications/ccsp/ccsp-self-study-resources.

[6] Amazon Web Services (AWS). n.d. *AWS CloudTrail API Reference.* https://docs.aws.amazon.com/awscloudtrail/latest/APIReference/Welcome.html.

[7] North American Electric Reliability Corporation (NERC). n.d. *GridEx.* https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx.

[8] M. Malatji, "Management of enterprise cyber security: A review of ISO/IEC 27001:2022," 2023 International Conference On Cyber Management And Engineering (CyMaEn), Bangkok, Thailand, 2023, pp. 117-122, doi: 10.1109/CyMaEn57228.2023.10051114.

[9] (2021). DevSecOps: Integrating Security into the DevOps Lifecycle for Enhanced Resilience. 6. 1-19.

[10] Tipton, Harold F., and Micki Krause. Information security management handbook. CRC press, 2007.

[11] NIST. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology, 2018, https://doi.org/10.6028/NIST.CSWP.29. Accessed 16 Oct. 2024.

[12] Idaho National Laboratory. n.d. *Malcolm.* https://malcolm.fyi/.

[13] Splunk. (n.d.). *Splunk.* Retrieved from https://www.splunk.com/

[14] Snort. n.d. *Snort.* https://www.snort.org/.

[15] Nessus. n.d. *Tenable Nessus.* https://www.tenable.com/products/nessus.

[16] Idaho National Laboratory. n.d. *All Hazards Analysis.* https://inl.gov/national-security/ics-aha/.

[17] Shodan. n.d. *Search Engine for the Internet of Everything.* https://www.shodan.io/.

[18] Maltego. n.d. *Maltego.* https://www.maltego.com/.

[19] CrowdStrike. n.d. *Falcon Platform.* https://www.crowdstrike.com/falcon-platform/.

[20] Idaho National Laboratory. n.d. *Cyber-Informed Engineering.* . https://inl.gov/national-security/cie/.

[21] Cybersecurity and Infrastructure Security Agency (CISA). n.d. *Known Exploited Vulnerabilities Catalog.* https://www.cisa.gov/known-exploited-vulnerabilities-catalog?page=1.

[22] Cybersecurity and Infrastructure Security Agency (CISA). 2023. *BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities.* November. https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-ex.

[23] Cybersecurity and Infrastructure Security Agency (CISA). n.d. *Downloading and Installing CSET.* https://www.cisa.gov/downloading-and-installing-cset.

[24] U.S. General Services Administration, "Federal Risk and Authorization Management Program (FedRAMP)," [Online]. Available: https://www.fedramp.gov/. [Accessed: Oct. 7, 2024].

[25] Cybersecurity and Infrastructure Security Agency (CISA). n.d. *Downloading and Installing CSET.* https://www.cisa.gov/downloading-and-installing-cset.

[26] National Institute of Standards and Technology (NIST). n.d. *NIST Cybersecurity Framework.* . https://www.nist.gov/cyberframework.

[27] National Institute of Standards and Technology, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82, Revision 2, Apr. 2015. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/82/r2/final. [Accessed: Oct. 11, 2024].

[28] Idaho National Laboratory (INL). n.d. *Critical Infrastructure Protection and Energy Assurance.* . . https://inl.gov/national-security/cie/.

APPENDIX

Results of the final generated PDF from Cirrus are subject to change based on the answered inputs. The examples included in this appendix represent a sample of the outcomes generated by Cirrus, while the final PDF will offer detailed insights based on actual data and use case inputs. Included in this appendix are examples of what is covered, but the full comprehensive PDF will include the following:

1. Introduction
2. Use Case
3. Identity and Needs Analysis Overview
4. Utility Goals for Modernization Scoring
5. Application Taxonomy and Decomposition Overview
    a. KPI Chart
    b. HCE Chart
6. Engineering Control Overview
7. Secure Information Architecture Overview
    a. Data Management
8. Strategic Roadmap
    a. Utility Risk Profile Chart
        i. Area/Load Impact, Duration. Breadth/Cascading Impact, Safety, Asset Owner/System Integrity, and Cost overview.
    b. Use Case Study based recommendations
9. Anticipated Benefits of Cloud Migration
10. Benefits vs. Risks of Cloud Migration
11. Request for Information & Guidance
    a. Team Contacts and Email: csdet.cloud@inl.gov

Cirrus

Cirrus Cloud Feasibility Study

The Department of Energy's Grid Deployment Office (DOE GDO) is spearheading a transformative initiative with Idaho National Laboratory to enable the seamless integration of cloud technology into the grid of the future. This project outlines a comprehensive roadmap to strategize, guide research, and facilitate the deployment of cloud solutions in the digital energy transformation within the electric and interconnected grid systems. By harnessing cloud solutions, and deploying responsibly and securely we aim to bolster grid resilience, future-proof its operation, and support the transition towards a decarbonized electric grid.

The purpose of this technical assistance program is to improve resilience in the grid modernization space with enhanced security programs. By guiding users through a tailored analysis and mitigation program to determine their current security posture, assistance in evaluating supply chain and protection choices against consequences and helping entities develop a future sustainable assessment and procurement planning system.

The technical assistant (TA) is designed to be responsive to a rapidly changing regulatory and policy landscape that seeks to match the timing and depth of questions with National Laboratory subject matter experts (SME) on key topical areas. This program augments and complements current technical assistance activities undertaken by various DOE program offices.

As part of this report you will find a strategic roadmap to help you understand your current status in cloud implementations. A list of steps your company could purse to continue with the transition will include as well as suggestions of third-party companies that may be worth reaching out to depending on your organization needs, national and local regulations needed to be address and security measures.

Use Case

The Cirrus framework is designed for teams considering either a transition or a first application in the cloud. This framework doesn't provide a definitive yes or no; rather, it offers strategic guidance on how to prepare for, or deploy, a cloud solution responsibly. While that is not the entire industry, in the initial stages of planning new applications or furthering a larger more-mature entity's strategy, consequence-based analyses provide an approach that can be communicated and discussed across senior leadership and the different technical levels of staffing.

This assessment provides the utility with a strategic roadmap for adopting cloud technologies, emphasizing a risk-informed approach to enhance operational resilience and efficiency. The output of this framework is a profile of the utility's risk, the benefits of cloud migration, the utility's readiness, and considerations it must understand before and during deployment (including potential costs and questions to be asked 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. 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. A workforce assessment will also be provided in the results to give an entity the capability of hiring or training appropriately capable staff. The framework is designed to facilitate the cloud migration of small-to-medium electric utilities in the United States. The assessment encompasses several critical dimensions to ensure a smooth transition and effective deployment.

Area/Load Impact:

- Latency: Increased latency due to geographic distance or network issues
- Resource Mismatch: Inadequate cloud resources leading to inefficiencies
- Scalability Issues: Performance bottlenecks due to insufficient scaling policy
- Overloading: Overwhelming the cloud infrastructure, causing performance issues

Duration:

- Extended Migration Time: Migration taking longer than expected
- Resource Contention: Contention for resources affecting both environments
- Complexity: Increased complexity and difficulty in managing longer projects
- Downtime: Significant disruptions to business operations due to prolonged migration

Breadth/Cascading Impact:

- Configuration Drift: Inconsistencies between environments causing issues
- Dependency Failures: Failures or degradation in interconnected systems due to dependency issues
- Service Interruptions: Widespread disruptions from changes affecting other systems
- Data Integrity: Data loss or corruption due to cascading impacts of the migration

Safety:

- Access Control: Inadequate access control exposing systems to unauthorized access
- Vulnerabilities: Security gaps or unpatched vulnerabilities in cloud services
- Compliance Issues: Legal and financial penalties from non-compliance with regulations
- Data Security: Potential exposure or inadequate protection of sensitive data

Asset Owner/System Integrity:

- Configuration Management: Inconsistent configurations causing performance and security issues

Data organization and security

- With the significant amount of data generated by improvement in grid technology, e.g. smart grids and sensor, the use of cloud allows for data storage, management and analysis. This information in so permits the reliability of the grid, optimize energy distribution and data driven decision, predictions and improvements.[1]
- By incorporating cloud utilities will have access to real-time data management that will help in planning and lowering cost of infrastructure maintenance.[2]

Collaboration

- The incorporation of cloud to your system, can give your company the opportunity to trade energy resources between consumers and other producers.[3]
- Cloud integration allows for collaboration with partners different regions, e.g. for remote monitoring, maintenance or control infrastructure. This benefits not only costs but also because given an emergency those remote partners can respond quickly and efficiently. There is also the opportunity to prioritize collaboration with other organizations that have aligning values.[1]
- Utilities understand to incorporate cloud to their companies they do not need to become a technology firm. With using cloud, they can focus more on their core strengths and less on technology infrastructure, not needing to meet all their technology needs because they can partner with technology firms to cover those needs.[2]

Improved demand response

- With cloud integration, companies and consumers can observe and manage their use in real time in so benefiting in lowering cost and promote efficient use of energy.[3]

Readiness Assessment

These recommendations are based on the overall preliminary metrics of the assessment, that is we will take into consideration based on your current cloud technology implementation:

Multi source data view

- ADMS give operators the actionable data they want for safer and more effective operations by assists in automating data assimilation. Operators may get the actionable information they want by combining the essential distribution operations of a SCADA system with outage management, switching, and network analysis and optimization tools into a single solution with a single pane of glass for distribution operations. Operations become safer and more effective when the ADMS helps send the correct data to the appropriate user at the right time.[4]

Model of Shared Distribution Network Operations

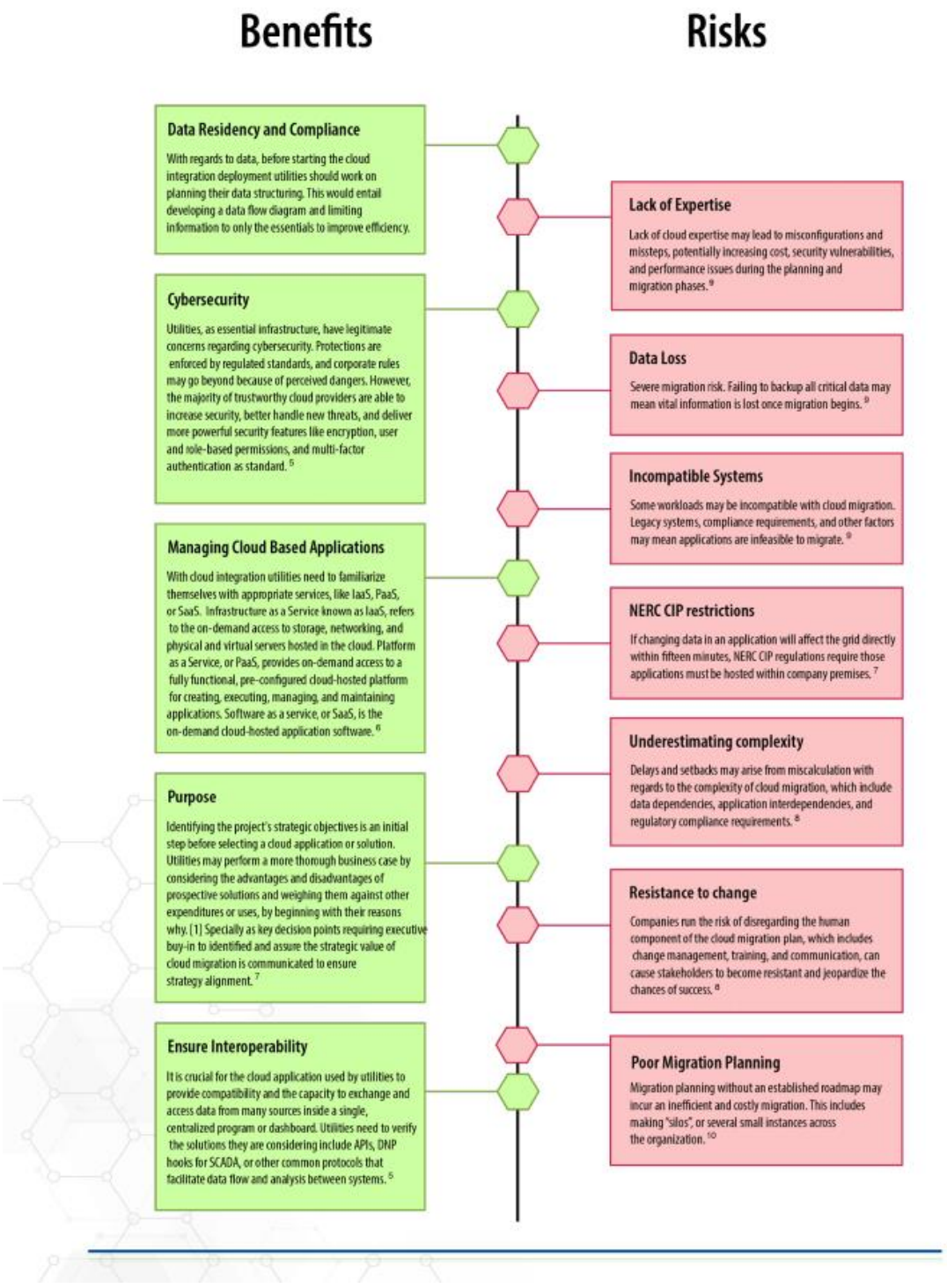
- More and more DERs are connected to the distribution grid. It takes a lot of work and resources to continually synchronize several diverse viewpoints of the distribution system with multiple digital solutions and apps. ADMS provides and efficient option to share Distribution Network Operations Model. Utilities will be able to concentrate on secure system supervision and control instead of handling data integration and synchronization [4]

Data Management

- A single individual cannot physically or financially manage to monitor, collect, and analyze data for every facet of the distribution network. Integration is required for data from smart field equipment, including Weather Data Services, Advanced Metering Infrastructure (AMI), Geographic Information Systems (GIS), and Customer Information Systems (CIS). System users gain situational awareness and the ability to utilize information to make better business choices when disparate forms of information are combined into a unified, understandable perspective.[4]

Outages Reaction

- Using an ADMS, utilities may evaluate proposed restoration actions to increase customer satisfaction and outage response efficiency, as well as immediately assess the magnitude of an unplanned outage. The full ADMS solution is performance-oriented, scalable, and secure—even when handling many outages at once. Through secure connections, field personnel are able to rapidly validate approved switching actions, access real-time data, and get optimal task allocation.[4]


Benefits
Risks
Data Residency and Compliance
With regards to data, before starting the cloud integration deployment utilities should work on planning their data structuring. This would entail developing a data flow diagram and limiting information to only the essentials to improve efficiency.
Cybersecurity
Utilities, as essential infrastructure, have legitimate concerns regarding cybersecurity. Protections are enforced by regulated standards, and corporate rules may go beyond because of perceived dangers. However, the majority of trustworthy cloud providers are able to increase security, better handle new threats, and deliver more powerful security features like encryption, user and role-based permissions, and multi-factor authentication as standard. [5]
Managing Cloud Based Applications
With cloud integration utilities need to familiarize themselves with appropriate services, like IaaS, PaaS, or SaaS. Infrastructure as a Service known as IaaS, refers to the on-demand access to storage, networking, and physical and virtual servers hosted in the cloud. Platform as a Service, or PaaS, provides on-demand access to a fully functional, pre-configured cloud-hosted platform for creating, executing, managing, and maintaining applications. Software as a service, or SaaS, is the on-demand cloud-hosted application software. [6]
Purpose
Identifying the project's strategic objectives is an initial step before selecting a cloud application or solution. Utilities may perform a more thorough business case by considering the advantages and disadvantages of prospective solutions and weighing them against other expenditures or uses, by beginning with their reasons why. [1] Specially as key decision points requiring executive buy-in to identified and assure the strategic value of cloud migration is communicated to ensure strategy alignment. [7]
Ensure Interoperability
It is crucial for the cloud application used by utilities to provide compatibility and the capacity to exchange and access data from many sources inside a single, centralized program or dashboard. Utilities need to verify the solutions they are considering include APIs, DNP hooks for SCADA, or other common protocols that facilitate data flow and analysis between systems. [5]
Lack of Expertise
Lack of cloud expertise may lead to misconfigurations and missteps, potentially increasing cost, security vulnerabilities, and performance issues during the planning and migration phases. [9]
Data Loss
Severe migration risk. Failing to backup all critical data may mean vital information is lost once migration begins. [9]
Incompatible Systems
Some workloads may be incompatible with cloud migration. Legacy systems, compliance requirements, and other factors may mean applications are infeasible to migrate. [9]
NERC CIP restrictions
If changing data in an application will affect the grid directly within fifteen minutes, NERC CIP regulations require those applications must be hosted within company premises. [7]
Underestimating complexity
Delays and setbacks may arise from miscalculation with regards to the complexity of cloud migration, which include data dependencies, application interdependencies, and regulatory compliance requirements. [8]
Resistance to change
Companies run the risk of disregarding the human component of the cloud migration plan, which includes change management, training, and communication, can cause stakeholders to become resistant and jeopardize the chances of success. [8]
Poor Migration Planning
Migration planning without an established roadmap may incur an inefficient and costly migration. This includes making "silos", or several small instances across the organization. [10]