NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

BES Operations in the Cloud

NERC Security Integration and Technology Enablement Subcommittee White Paper

September 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

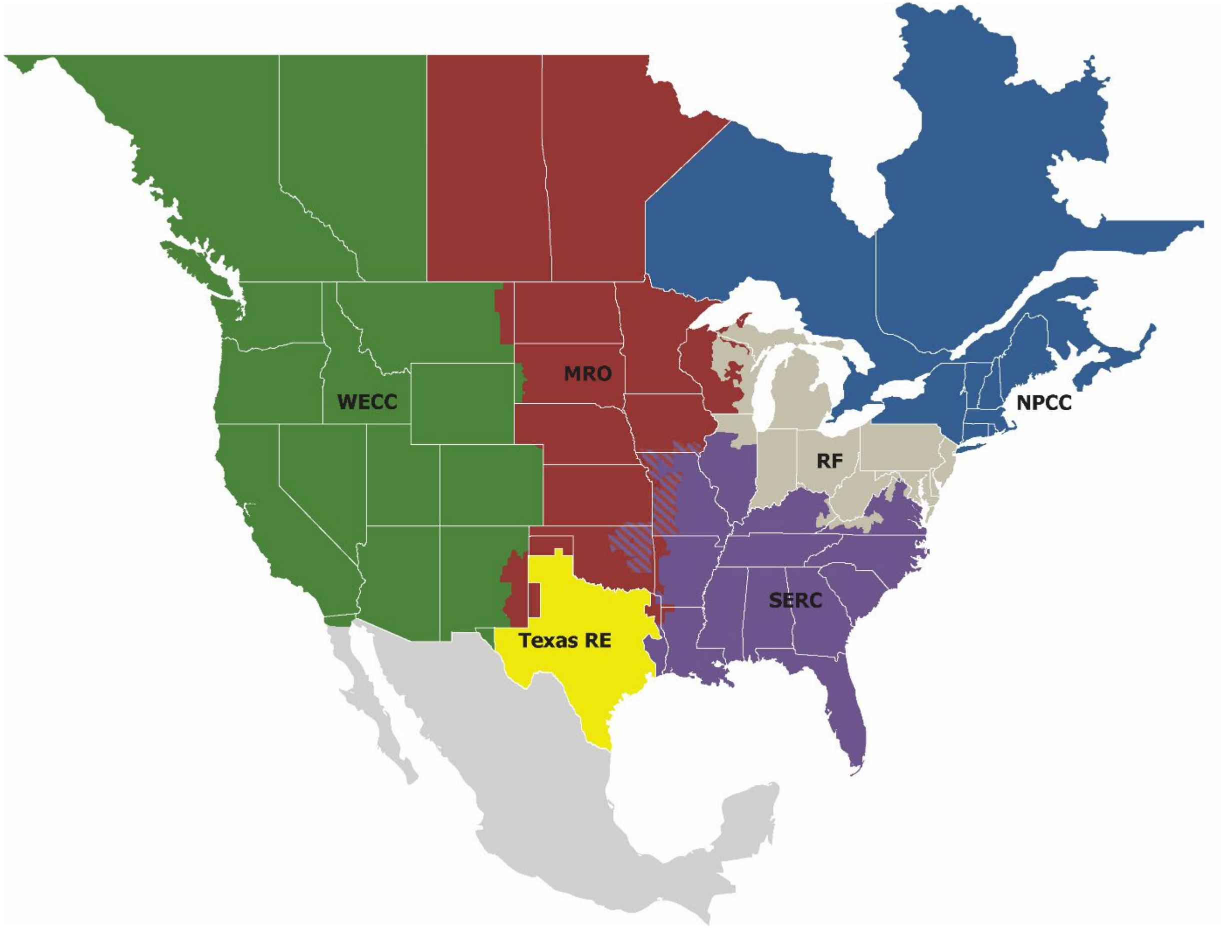
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

Disclaimer

Reliability Guidelines, Security Guidelines, Whitepapers, and Technical Reference Documents suggest approaches or behavior in a given technical area for the purpose of improving reliability. Whitepapers are not mandatory requirements or binding norms. Instead, they explore technical facets of topics and do not create mandatory Reliability Standards.

The exploration of cloud-computing use cases in this whitepaper is not to be construed as NERC or Reliability and Security Technical Committee (RSTC) endorsement of any particular use-case for cloud-computing, nor an endorsement of any vendor offering services or solutions related to such use cases.

This whitepaper and the recommendations herein do not reflect RSTC endorsement of any SAR, which may have been developed by a non-RSTC entity.

The choice to evaluate cloud computing use cases and make the business decision to move any piece of an operational or supporting function to a cloud-based solution rests solely in the hands of each individual entity. This whitepaper does not constitute a position on that decision.

The Security Integration and Technology Enablement Subcommittee (SITES) recognizes industry's innovative spirit in exploring the value presented by cloud computing technology for various applications in support of the Bulk Electric System (BES). Innovative offerings from vendors within the electric sector are steadily including virtualization and cloud solutions. However, utilities should carefully assess security and reliability risks of migrating systems and applications associated with BES reliability operating services (BROS) to the cloud, especially those critical systems with high availability requirements. SITES identifies that BES operations are broad, and there are many opportunities for large data analysis and systems that are not real-time to benefit from cloud services.

SITES intends to enable the use of the cloud for registered entities but acknowledges that it is ultimately up to individual entities to determine their business objectives, and both operational and technology requirements in determining any use cases that may be right for them. SITES strongly recommends that registered entities take a gradual approach to cloud migration by starting with information technology (IT) and non-regulated workloads. Entities should approach cloud migration cautiously for real-time and critical BES field and operations applications and ensure that the entity reaches maturity in its knowledge and capabilities with cloud technology, can verify cloud and application architectures to achieve that entity's requirements for reliability and security, and that the entity is prepared and informed to tackle compliance challenges. Furthermore, SITES recognizes challenges associated with resolving regulatory compliance to NERC Critical Infrastructure Protection (CIP) Reliability Standards for BES operations hosted in cloud service provider (CSP) environments as a barrier to cloud adoption within the industry. SITES has identified the need for enhancements to the basis and capacity for ERO Enterprise auditors to accept the work of others with regards to third party certification of CSPs to cloud security frameworks, and independent cloud risk assessments from registered entities with the end goal of aiding in evidencing NERC CIP compliance of BES operations hosted within CSP clouds.

Introduction

The electric grid industry is entering a new era of digital transformation and driven further by the adoption of cloud computing technology. With the potential to enhance the efficiency, resilience, and innovation of the Bulk Electric System (BES), cloud technology presents an opportunity for industry stakeholders to modernize BES reliability operating services (BROS). However, adopting cloud technology for BES operations comes with challenges, including regulatory compliance, security, and reliability concerns. This white paper aims to explore these challenges and opportunities while educating and providing guidance to entities to better navigate these complexities and make informed decisions about cloud adoption. Examination of business drivers, core concepts, and industry use cases as well as key recommendations to address regulatory constraints make up some of the valuable content found herein.

FERC Order

In December 2020, in an order regarding virtualization and cloud computing services, the Federal Energy Regulatory Commission (FERC) directed NERC "to begin a formal process to assess the feasibility of voluntarily conducting BES operations in the cloud in a secure manner." The order discussed industry comments, including those submitted by NERC, which suggest that using cloud computing services could be expanded for purposes other than BES Cyber System Information (BCSI) storage, including the nine BROS,[1] so long as the risks associated with these technologies are carefully addressed. Evaluating these risks and weighing them against the potential cost savings, enhanced security, and operational resilience is key to developing an effective path forward regarding any additional modifications to the CIP Reliability Standards. In December 2022, NERC made its informational filing regarding BES operations in the cloud. SITES has developed this white paper to further the assessment of securely conducting BES operations in the cloud and to provide industry with clear technical guidance on this topic.

This white paper focuses on the use of cloud computing technologies for BES operations. It builds on past work in the areas of cloud technologies particularly related to storing and accessing BCSI (i.e., "data in storage" and "data in transit"). The FERC directive focuses directly on BES operations using cloud technology (i.e., "data in use"); hence, the goal of this white paper is to provide technical content, findings, and recommendations on this subject.

Related Efforts

Several NERC projects, and other industry stakeholder group work products, exist with relation to virtualization and cloud computing. BCSI in particular has received focus over BES operations. Industry comments in response to the February 2020 FERC Notice of Inquiry (NOI) regarding virtualization and cloud computing for BES operations showed some entities have been voluntarily using virtualization and cloud hosting regarding data storage of BCSI. NERC Project 2016-02 and Project 2019-02 are expected to facilitate the use of virtualization and cloud computing for BCSI and clarify any uncertainties regarding compliance risks associated with using virtualization.

The following efforts and work products are related to virtualization and cloud computing:

- *NERC Standards Project 2016-02: Virtualization*
- *CIP V5 Transition Advisory Group (V5 TAG) White Paper*
- *NERC Standards Project 2019-02: BCSI Access Management*
- *NERC Compliance Monitoring and Enforcement Program (CMEP) Practice Guide: BES Cyber System Information*
- *NERC Security Guideline: Supply Chain Risks Related to Cloud Service Providers*
- *FERC NOI on Virtualization and Cloud Computing Services*
    - Comments on *FERC NOI on Virtualization and Cloud Computing Services*

[1] See **Appendix B:Explanation of BROS and CIP-002-5.1a**

Intended Audience and Scope

This white paper focuses on applications of cloud technology in the electricity sector suitable for TOs, TOPs, Transmission Planners (TPs), Planning Coordinators (PCs), Reliability Coordinators (RCs), Balancing Authorities (BAs), Generator Owners (GOs), Generator Operators (GOPs), Distribution Providers (DPs), and others. The discussion includes use cases in real-time environments (i.e., operations within 15 minutes), near-real-time control center functions, field applications, and engineering tools for long-term planning and other functions. This white paper is intended for the following:

- Power and utility senior leaders, engineers (operations, planning, system architecture, etc.), cyber security professionals, and compliance teams
- Independent software vendors
- Cloud service providers
- Systems integrators
- Regulatory bodies and policymakers

Drivers for Electricity Sector Adoption of Cloud Technology

The electric delivery landscape is changing, prompting operators to adapt. There are numerous drivers for adoption of cloud technology, many of which are applicable to NERC registered entities and the electricity sector. Among the drivers include the following:

- **Changing Resource Mix:** The changing resource mix towards increasing levels of variable energy resources and distributed energy resources (DERs) is causing more variability and uncertainty on the BPS today and into the future. Entities need faster, smarter and more automated analytics tools for engineering and real-time operational decisions.
- **Digitalization:** The advent of microprocessor-based devices[2] across the entire electricity ecosystem is providing entities with massive amounts of data. While this data can improve situational awareness, decision-making, asset management, and support many other business decisions, most of the data is used ineffectively or completely unused because of the computational burden. Cloud technology offers unique opportunities to leverage data more effectively and efficiently.
- **Resilience:** Cloud infrastructure could support a resilient energy infrastructure by enabling multi-region data storage and computing power that is highly dispersed geographically and highly redundant. This may help with business continuity plans, incident response, disaster recovery (natural or human-made), and other key business needs.
- **Advanced Analytics:** With all this data, entities are constantly focused on improving business decisions—better long-term planning and asset management decisions, more accurate and effective operational decisions, and better situational awareness. This requires advanced analytical tools that can leverage the increase in available data. Software vendors, solutions architects, and systems integrators need to ensure that data storage tools, applications, and front-end tools are able to leverage the data effectively. This presents challenges for the utility industry—whose tools and applications typically use legacy protocols and standards due to the long lifetime of different types of assets on the system. Cloud computing can unlock new decision frameworks and advanced algorithms, such as including machine learning and artificial intelligence.

[2] This could include microprocessor-based relays, remote terminal units (RTUs), phasor measurement units (PMUs), advanced metering infrastructure (AMI), smart meters, the Internet of Things (IoT), and many other forms measuring devices in generation, transmission, and distribution environments.

- **Widespread Adoption of Cloud Technology in Other Sectors:** Many other industries have moved toward the use of cloud technology in different forms, including other critical infrastructure (e.g., financial services, healthcare, life sciences). Many solutions providers, software vendors, and other third-parties offer cloud technology solutions. As providers continue to innovate and shift to cloud-first approaches, on-premises solutions may be discontinued or may be unable to meet the needs of utilities.

- **Managing Costs:** With the cross-sector movement toward cloud technology offerings, it may become cost restrictive to continue using more legacy tools and approaches in the future since technology providers would need to create "one-off" solutions for utilities. Therefore, entities will need to balance costs while ensuring sufficient reliability and security of their systems.

- **Available Expertise and Resources:** The rapid technology evolution is creating challenges of obtaining and retaining highly skilled security professionals in the electric sector broadly. Cloud security is increasingly a part of cyber security training curricula for security professionals graduating today and in the future. It will become increasingly difficult to find skilled professionals that understand legacy systems and security measures, which makes finding individuals with the necessary skills in cloud security and legacy systems a challenge as well.

- **Focus on Core Business Activities:** Use of cloud infrastructure, services, and expertise enables utilities to focus on core business activities rather than time-consuming administrative tasks, such as provisioning hardware and managing IT infrastructure. Utility IT and security professionals are able to focus more heavily on securing the systems and critical infrastructure under their responsibility rather than managing networks and systems.

Chapter 1: Overview of Cloud Computing for BES Operations

Cloud Technology Service Models

"Cloud computing" generally refers to on-demand delivery of information technology (IT) resources via the Internet with scale-on-demand resources and pay-as-you-go pricing. Instead of buying, owning, and maintaining data centers and servers, organizations acquire technology (computing power, storage, databases, and other services) on an as-needed basis. CSPs manage and maintain the infrastructure and access to these resources for their customers to develop and run applications. However, the term "cloud" is not a standardized definition. Cloud technology embodies a range of technological capabilities of which data center infrastructure is just one component. CSPs may offer one or more service models presenting different capabilities to meet different business and operational needs of their customers as shown in Figure 1.1. Cloud technology and service offerings include the following:

- **Infrastructure as a Service (IaaS):** A cloud computing service where customers rent or lease servers for computing and storage in the cloud. This eliminates the need to manually provision and manage physical on-premises servers in data centers. Most operating systems or applications can be run on the IaaS.
- **Platform as a Service (PaaS):** A category of cloud computing services that allows customers to provision, instantiate, run, and manage a modular bundle that is comprised of a computing platform and one or more applications. This is done without the complexity of building and maintaining the infrastructure typically associated with developing and launching the applications. As a result, this allows developers to create, develop, and package such software bundles.
- **Software as a Service (SaaS):** A software distribution model in which CSPs and independent software vendors (ISVs) offer applications that are hosted in the cloud and makes them available to end users over the internet
- **Hybrid Cloud:** An option where servers can be deployed at on-premises data centers to run various services offered by the CSP. This creates high speed, local compute capabilities and off-site redundancy and backup. This allows users to distribute their workloads between on-premises and cloud infrastructure based on their needs.

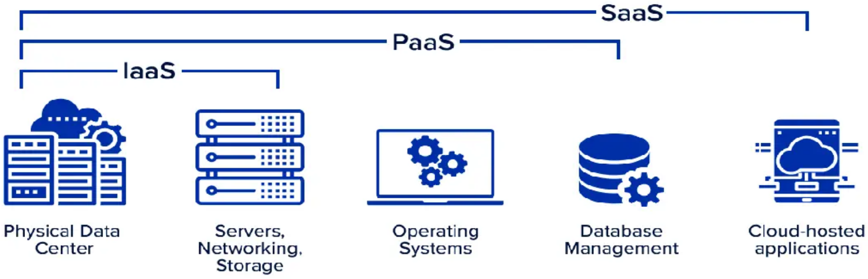


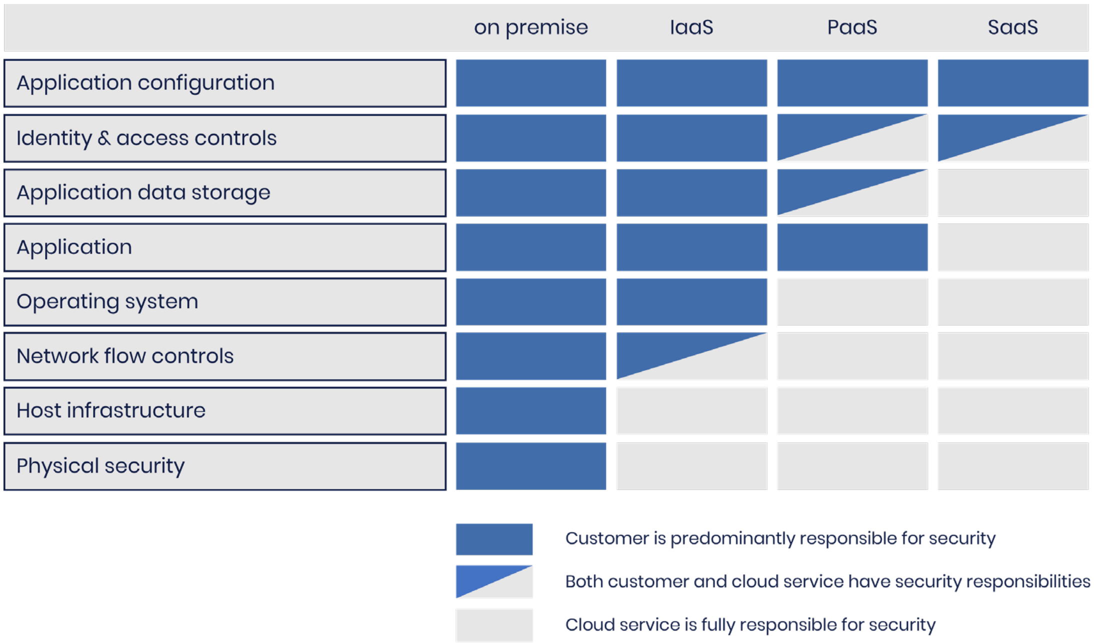
Figure 1.1: Cloud Service Models

The terms "underlay" and "overlay" are commonly used to establish a helpful abstraction between systems provided and supported by the CSP within a given service model versus the systems or applications built and/or configured by the customer within the hosted cloud environment. The underlay represents all components managed by the CSP, and the overlay represents the components managed by the customer and essentially built on top of the underlay. For example, in an IaaS model, the overlay includes any systems built by an entity within the provided virtual environment. Whereas in a SaaS model, the overlay may simply be the entity's data and configurations within a hosted application. These terms help create further clarity when leveraged in the discussion of responsibility for securing the cloud environment and cloud hosted systems.

Shared Responsibility Model

In a typical on-premises security model, customers are responsible for the end-to-end security in their data centers. When working with a cloud service provider, security and compliance is a shared responsibility between the cloud service provider and the customer. This shared model can help relieve the utility’s operational burden as the CSP is responsible for the operation, management, and controls from the physical security of the facilities in which the service operates up to the host operating system and virtualization layer. In the case of PaaS and SaaS models, the CSP’s responsibilities may extend further.

In an IaaS service model, the registered entity assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of security tools provided by the CSP such as firewall rules. Utilities should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their on- premises or other cloud environments, and applicable laws and regulations. This differentiation of responsibility is commonly referred to as Security “of” the Cloud versus Security “in” the Cloud.



	on premise	IaaS	PaaS	SaaS
Application configuration	■	■	■	■
Identity & access controls	■	■	◩	◩
Application data storage	■	■	◩	□
Application	■	■	■	□
Operating system	■	■	□	□
Network flow controls	■	◩	□	□
Host infrastructure	■	□	□	□
Physical security	■	□	□	□

■ Customer is predominantly responsible for security

◩ Both customer and cloud service have security responsibilities

□ Cloud service is fully responsible for security

Figure 1.2: Shared Responsibility Model

CSP Responsibility “Security *of* the Cloud” or “Underlay”

CSPs providing IaaS are responsible for protecting the infrastructure that runs all of their cloud services. This infrastructure is composed of the hardware, software, networking, and data center facilities that run the cloud services. CSPs providing PaaS and SaaS services can be responsible for securing the operating system, data, and even application layer. ISVs offering PaaS and SaaS products may build upon their own infrastructure or host their services on other CSP infrastructure offered as IaaS. In those instances, from the customer or registered entity’s perspective, the ISV is the ultimately responsible party for ensuring protection of the complete cloud underlay including infrastructure. The ISV is party to the customer or registered entity’s contract agreement or service level agreement (SLA).

Entity Responsibility “Security *in* the Cloud” or “Overlay”

Registered entity responsibility will be determined by the CSP and cloud services that they select as a customer. This determines the amount of configuration work the customer must perform as part of their security responsibilities. It may be necessary for the entity to procure and implement their own security tools for systems built within the cloud overlay, such as the deployment of endpoint detection response (EDR) or network detection response (NDR) agents. Alternatively, security tools may be provided and built-in to the services provided by the CSP within the cloud. In such cases there is a shared responsibility of the security controls; the CSP's support of the tool within the underlay, and the entity's control configuration with the tool within the overlay. E.g., a virtual software firewall provided by an IaaS CSP and configured by the entity to perform traffic flow control, or application access roles provided by a SaaS vendor and configured by the entity for identity and access management.

The concept of shared responsibility should also be considered when obtaining security assurances through the acceptance of certifications and accreditations regarding the security of a cloud service provider or vendor leveraging a cloud service provider's products or services. Utilities should ensure that contractual agreements are in place regarding items such as certifications, accreditations, and security controls, and that they are well understood by all parties.

Inherited Controls, Certifications and Accreditations

A key consideration in assessing and selecting a CSP is the security and compliance status of their services. This can be evaluated by assessing their certifications and accreditations. There are various certifications and accreditations a CSP can obtain to demonstrate that they can "secure the cloud." These may include any or all of the following:

- FedRAMP Moderate and High (United States federal government standards)
- DoD (US Department of Defense) SRG
- PCI (Credit card processing)
- HIPAA (healthcare and medical record processing)
- SEC (securities and exchange commission) standards

In addition, CSPs may meet various security and process requirements including:

- SOC 1, 2, and 3
- ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 9001:2015,
- CSA STAR CCM v3.0.1

To maintain certification and accreditation to these security and compliance requirements, CSPs are often being continuously audited. These controls are audited by independent third parties with cloud security expertise. CSPs providing any cloud service model should be able to provide their set of accreditations to utilities to ensure their services achieve the required security control objectives. Selection of a vendor or their cloud services that do not match an entity's requirements will result in elevated security or compliance risk for that entity unless alternate steps are taken to mitigate the residual risk.

Shared Security Assurance

Similar to the shared responsibility model, entities should understand their responsibility for assuring security and compliance of systems hosted within a CSP's cloud environment. Registered entities have responsibility for any internal or external audits, including NERC CIP for any BES systems or BCSI leveraging CSP services. Additionally, due diligence by registered entities should involve periodic verification (trust but verify) that CSP certification is still in place.

It should be further noted that PaaS or SaaS vendors which are reliant on a separate IaaS provider may need to achieve and maintain specific certification or accreditations to match those held and attributed to the IaaS platform.

For example, a large CSP may provide a FedRAMP Moderate certified IaaS underlay, but a dependent software vendor may fail to acquire or maintain FedRAMP Moderate for their SaaS applications built on top in the overlay. In such a case, to claim FedRAMP Moderate certification, the software vendor would need to seek FedRAMP authorization for the SaaS application independent of the CSP for the controls that are the software vendor's responsibility. Figure 4 provides a major CSP example of the shared responsibility for security compliance assurance.

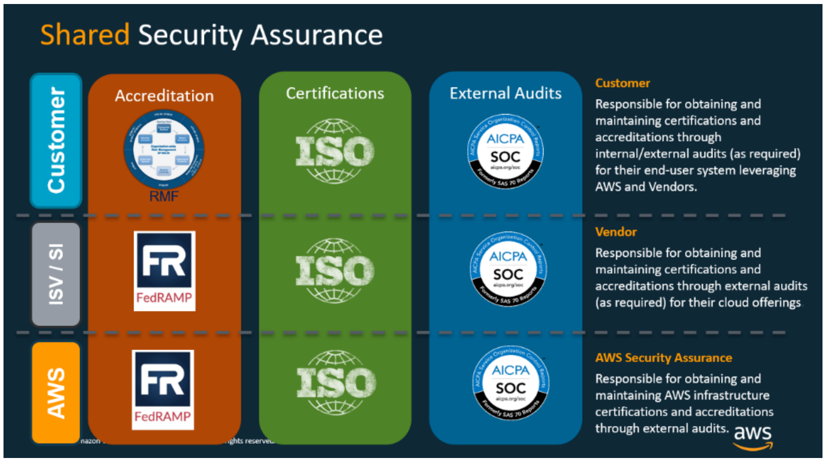
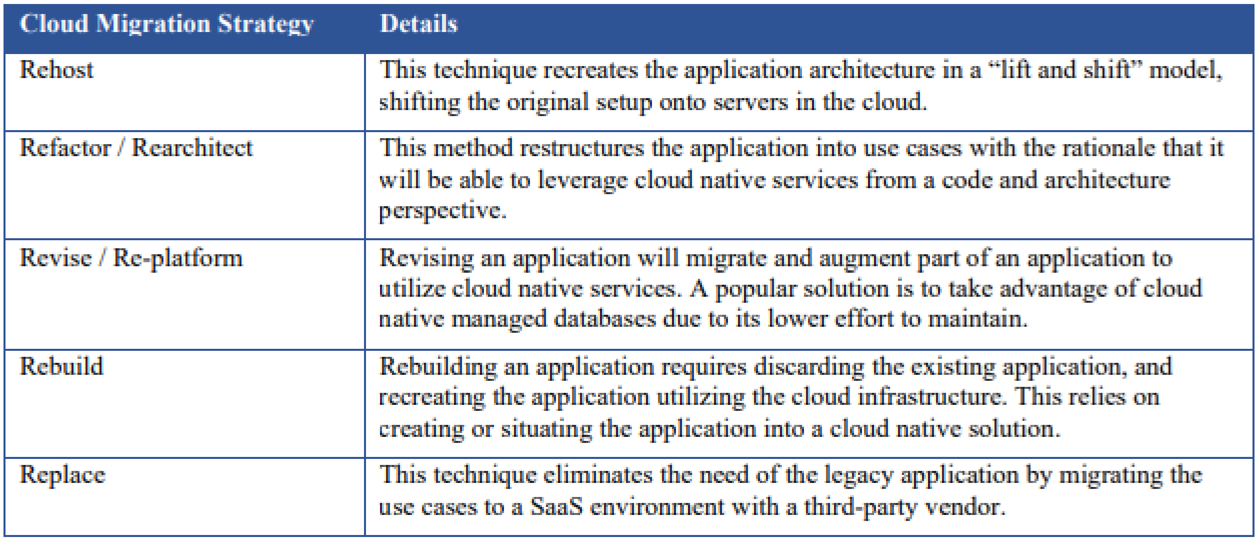

Shared Security Assurance
Customer
ISV / SI
AWS
Accreditation
Certifications
External Audits
RMF
FR
FedRAMP
ISO
AICPA
SOC
Customer
Responsible for obtaining and maintaining certifications and accreditations through internal/external audits (as required) for their end-user system leveraging AWS and Vendors.
Vendor
Responsible for obtaining and maintaining certifications and accreditations through external audits (as required) for their cloud offerings
AWS Security Assurance
Responsible for obtaining and maintaining AWS infrastructure certifications and accreditations through external audits.
aws

Figure 1.3: Shared Security Assurance for Amazon Web Services (AWS)

Cloud Migration Strategies

Moving system functions and operations into the cloud can be a daunting prospect for utilities when faced with the myriad of options presented by software vendors, system engineering professional services, as well as cloud service provider offerings. Understanding business and technical requirements, constraints such as aging on-premises infrastructure and limited staff knowledge and experience, or challenges like change management and funding should all play a part in the selection of a cloud migration strategy. Entities may adopt multiple strategies to fit different projects and different applications. CISA provides a wealth of technical information to assist with cloud migration in their published Cloud Security Technical Reference Architecture[3] which utilities may find useful as they take on this challenge. The common cloud migration strategies are listed in Figure 5.



Cloud Migration Strategy	Details
Rehost	This technique recreates the application architecture in a "lift and shift" model, shifting the original setup onto servers in the cloud.
Refactor / Rearchitect	This method restructures the application into use cases with the rationale that it will be able to leverage cloud native services from a code and architecture perspective.
Revise / Re-platform	Revising an application will migrate and augment part of an application to utilize cloud native services. A popular solution is to take advantage of cloud native managed databases due to its lower effort to maintain.
Rebuild	Rebuilding an application requires discarding the existing application, and recreating the application utilizing the cloud infrastructure. This relies on creating or situating the application into a cloud native solution.
Replace	This technique eliminates the need of the legacy application by migrating the use cases to a SaaS environment with a third-party vendor.

[3] https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf

Figure 1.4: Cloud Migration Strategies from CISA Cloud Security Technical Reference Architecture v2.0

Communications Links

Utilities considering migration of critical services to the cloud should carefully consider their connectivity requirements with the cloud environment. As a best practice rule, when evaluating the migration of any systems to the cloud, the level of network redundancy maintained for an on-premises configuration of the same system should become the baseline of redundancy for connectivity between on-premises datacenters and the cloud environment that will house the migrated system. For example, if there is N-1 redundancy for networking between control centers and a data center hosting an EMS system, then it may be justifiable for EMS system components migrated to the cloud to be supported by N-1 or greater redundancy of communication links between the end users and the cloud.

As there are multiple choices of cloud technologies to meet a utility's operational needs, entities also have multiple choices to communicate with the cloud environment through a variety of communications network options such as public Internet, dedicated cable, private fiber, 4G/5G wireless, and satellite. Achieving the necessary redundancy and resiliency of communications between an entity and the CSP cloud environment may involve leveraging multiple communications mediums by working with multiple telecommunications companies. Private dedicated bandwidth fiber connections between entity data centers to large CSP clouds may offer state-of-the-art security (e.g., IEEE 802.1AE MAC Security Standard (MACsec) encryption for 10Gbps and 100Gbps connections), allowing for natively encrypted, high-speed, dedicated communications.

Chapter 2: Assessing Security of BES Operations in the Cloud

Quality of Service and Resilience

Quality of service (QoS) is a description or measurement of the overall performance of a service, particularly as experienced by the users of the network. Understanding operational requirements is critical when assessing possible cloud migration. Types of operational requirements for quality of service include, but are not limited to, the following: availability, latency, throughput, criticality, redundancy, failure rate, recovery time, etc. These operational requirements determine how a possible cloud solution will be architected. This information influences resilient architecture design including possible use of redundant communications paths, private networks, multi-region cloud architecture, and other factors. Utilities should consider service level agreements (SLAs) and service level objectives (SLOs) that commit cloud service providers to providing a certain level of service. Utilities can review SLAs and SLOs by service against the operational requirements for their workloads to help determine if the services can meet the needs of each use case. When considering service requirements, utilities should also recognize that their architectural decisions play a role in meeting their operational requirements.

The reality is that CSPs large and small can experience outages, therefore, this must be part of a utility's equation for resiliency and business continuity needs. Consideration should be given to the overall architecture of the application(s) and how high-availability and redundancy is achieved relative to operational or business requirements. Larger scale or critical systems may need architectures to mitigate against regional disturbances by use of multi-region or hybrid cloud failover. For example, a utility may utilize both cloud hosted and on-premises server(s) in an active primary/backup configuration for a critical application or utilize one location as a live backup for disaster recovery.

Data Residency

CSPs may allow customers to choose and control the geographic location(s) among CSP data centers where their data will reside physically. For example, customers may be able to select which regions or areas that their data will be stored and the CSP will not move customer data without customer consent or request. These residency restrictions may include limiting to Registered Entity's country (or countries, depending on entity), however this should be carefully considered[4]. The registered entity needs the capability to fully assess and manage the residency of its data. Contractual and technical protections should be in place to ensure that data is held within these areas when selected by the entity. For national security reasons, wherever possible, BCSI information should reside within the country's boundary for which that entity operates. In cases such as an ISO/RTO that spans multiple countries while their members do not, open dialogue should be conducted between entities to form an agreement on data handling policies.

Security Objectives

Registered entities interested in migrating BES operations to the cloud should consider a number of security objectives to ensure availability, integrity, and confidentiality of the systems and applications trusted to the CSP's hosted cloud environment. Security objectives may differ based on the cloud service model and application use case at play. Entities should ensure controls are in place to meet the following non-exclusive list of priority security objectives are achieved either through tools provided in the overlay by the CSP, or procured and implemented by the entity within the cloud overlay (and on-premises) when necessary:

- Securing cloud to on-premises communication, including encryption and authentication
- Security logs and monitoring
- Data protection and data recovery including backups for servers, databases, or unstructured file data

[4] For example, Ukraine's law change in 2022 to allow government data and some private sector data to be hosted outside its own country allowed for the imminent backup of critical data during military invasion by Russia.

- Identity and access management
- Vulnerability management tools including patching and vulnerability scanning
- Malicious code detection or prevention
- Network security including IPSec VPN, access control lists, and secure service gateways

The Security Working Group (SWG) in collaboration with NERC, the ERO, and Azure performed an audit tabletop of BCSI in the cloud. They have produced a technical reference package that includes tabletop findings, lessons learned, completed practice RSAWs, as well as a risk evaluation with contract considerations of data handling, recovery, and protection controls. The technical reference package is expected to be published in Q2 2023.

Evaluation Criteria for Selecting CSPs and Cloud Services

Registered entities should establish evaluation criteria, at the beginning and then as new information is captured, to ensure relevant factors are considered. During the cloud service provider selection process, new information may continually come to light as options and technology evolve. An organization should develop criteria for its evaluation process that captures business objectives, organizational use cases, technical requirements or restrictions, QoS requirements, and security and compliance needs including data residency, protection, and recovery. The following sections explore topics for consideration during CSP evaluation.

Use Cases & Business Justification

Defining IT and OT use cases in advance provides an opportunity to organize and define a roadmap for adoption. Selecting the appropriate cloud service provider that can support the majority of the key roadmap deliverables will be key to creating a sustainable cloud integration and implementation program.

An example of use cases that support successful adoption may include starting with IT and non-regulated workloads first. IT and OT business teams can become more aware of core functionality, opportunities and features without risking compliance and regulatory challenges. Workloads that may be appropriate include drone video storage, vegetation management, alternative energy management, remote non-regulated workloads, outage management systems, asset management and training environments. Presently, vendors already offer cloud-based solutions for many of these use cases today.

Future-looking business-related factors such as mergers and acquisitions should be considered early when developing business cases for cloud adoption. Additionally, developing cloud infrastructure may position an entity for new lines of business, increase talent draw, and offer beneficial tax opportunities.

As we look at the business elements, some cloud service provider use cases can help entities’ structure the deals to support emerging financial models. With capital expense (CapEx) models, entities may be able to support the investment with their Public Utilities Commission versus an operating expense (OpEx) model, by including support, development and a longer-term infrastructure. Using the business case to present cloud adoption as a factor in improving grid reliability, security, and resiliency may allow for rate basing the technology investments alongside system infrastructure projects.

Integration with Existing Technology

Additionally, registered entities with existing IT Cloud products and services may want to evaluate and assess the ease of integration with existing cloud infrastructures, applications, or services.

Existing infrastructure constraints, such as those associated with on-premises assets and data centers, need to be evaluated for connectivity, transition support and decommissioning. Current technology contracts, administration, licensing and support are important considerations on the timing and flexibility options available to registered entities on their roadmap to cloud adoption. By leveraging cloud, migrations from legacy platforms and systems can be conducted quickly in concert with the cloud service provider. When configured properly, cloud solutions can help set up the entity for future-proof system evolutions.

Telecommunication Infrastructure

Telecommunication infrastructure options play a key role in evaluating bandwidth and resiliency requirements. Extending the enterprise local-area network (LAN) to the cloud may streamline connections for on-premises users. Site-to-site communications may be more efficient because they allow entities to connect straight to the cloud environment rather than having dedicated circuits connecting back to the main headquarters or communications hub. Reducing dependencies on any one location may provide greater flexibility and resiliency should the main location suffer a communications failure. In this way, should there be an interruption, data and information can continue to be gathered, and command and control of remote sites can be maintained. Additional benefits may be realized by reducing the bandwidth usage and providing more predictability in sustaining costs of dedicated corporate internet access.

Telecommunications requirements for real-time monitoring and alerting create inflexible dependencies on corporate networks. Developing alternative data paths and utilizing hybrid architecture leveraging cloud-based edge devices may facilitate cloud adoption solutions for real-time and field use cases.

Compliance Requirements

Entities using cloud-based solutions or CSP services need to ensure that the entity's NERC CIP requirements as defined by their entity registration, BES cyber system impact category, and other compliance requirements, can be met. Additional compliance may consist of customer and employee privacy, HIPAA, PCI, PRIEDA, CESA and State Privacy laws. Entities should evaluate other regulations and statutes that are relevant to their business and geography.

Other Considerations for CSPs and Cloud Services

- *Mobile workforce teams* such as deployment, maintenance or other crews may be able to connect to the cloud for work orders, designs and other necessary information easier than depending on corporate remote access solutions.
- *Remote workforce employees* may benefit from access to cloud hosted applications, shared data, dashboards, and virtual workspaces. CSPs can offer and support various connectivity methods and security protocols to facilitate these solutions. Hosting shared information in the cloud may provide for faster response and access for those on limited bandwidth connections while reducing corporate Internet bandwidth consumption.
- *Authentication schema support*, such as LDAP and Active Directory, can be provided by CSPs to host or extend authentication to cloud infrastructure to provide redundancy or facilitate single sign on and other benefits.
- *Training* is a key element for registered entities that are looking to integrate cloud infrastructures, software, and services into their environment. CSPs that offer online, or in-classroom training and comprehensive support programs may be better suited for new internal IT and OT teams looking to adopt their technologies.

Cloud Risk Assessments

Any registered entities wanting to evaluate migration of BES reliability operating services or supporting services to a cloud platform, should conduct their own reliability risk assessments. As such services are commissioned, applicable risks would then move to the registered entity's ongoing risk management plan or process. Generic cloud service risk assessment frameworks and guidance for entities to consider are presently available from sources such as the National Institute of Standards and Technology (NIST). Where applications and services support BES operations, risk management plans for cloud adoption should be expanded to include risk items for grid reliability and compliance management. Other risk factors may include the diversification of service providers or service technologies, integrations between applications hosted in different cloud environments, as well as significant reliance on a single CSP. Finally, as new cloud-based technologies and services emerge these risk profiles may change, and ongoing monitoring of evolving risks will be needed at regular intervals.

A risk management structure that appropriately segments and clearly demarks risk ownership between registered entities and cloud service provider is critical to success. Responsibility matrices are one tool to assign responsibilities. Enforcement of ownership can be achieved via contractual agreements and possibly monitored using technical or administrative methods. NIST discussed the key provisions for a framework for [5]Managing Risk the Cloud.

[5] Chapter 7: Managing Risk in the Cloud (nist.gov)

Chapter 3: Examining Use Cases in the Electricity Sector

This section elaborates on possible use cases of cloud technology in different environments used by various NERC registered entities. This list is not intended to be comprehensive, nor is it intended to provide all operational challenges or risks associated with each use case. It is, however, intended to illustrate the many different ways in which cloud computing *could* be used moving forward.

Long-Term Planning Applications

The primary benefits of leveraging cloud technology in the long-term planning horizon include increasing study workloads and reducing costs. With the increasing complexity and rapid integration of new BES resources, transmission planners are faced with performing increasing number and complexities of studies in a shorter timeframe. Cloud technology can help support reduced costs of executing those studies by leveraging shared computational resources off-site rather than the entity maintaining sufficient on-premises resources to meet peak demand in a timely fashion. This is particularly important during the interconnection study process where very short timelines are allotted to execute these types of studies. Examples of workloads in the long-term planning horizon (both planning assessments and interconnection studies) where cloud technology may provide benefits include:

- Improving development, maintenance, and utilization of network models and updates to those models
- Reducing equipment overhead costs by leveraging shared cloud resources for storage and computation of study work
- Increasing the number of base cases and operating conditions studied
- Increasing the number of sensitivity cases performed
- Increasing the number and depth of contingencies applied (e.g., N-1-1 analysis)
- Performing electromagnetic transient (EMT) studies during interconnection studies
- Performing EMT studies during annual planning assessments
- Increasing the number of EMT studies executed for any given project or network being studied
- Enabling the executive or monitoring of reliability studies from anywhere at any time

Other types of functions performed by planners and associated departments could include:

- Storage and management of drawings, procedures, calculations, and relay/PLC configuration files
- Effective development and deployment of asset management plans
- Coordination and collaboration between engineering, technician, construction and field support staffs

The NERC CIP Standards are generally not applicable to the long-term planning horizon since these activities do not have an operational impact within a 15-minute time horizon. Furthermore, planning studies generally do not include data that would be considered BCSI, although each entity would need to determine this for their organization.[6] Other designations such as Critical Energy Infrastructure Information (CEII) may impose additional confidentiality requirements to this type of information that would need to be handled accordingly. Therefore, entities need to ensure an adequate security posture in the cloud environment that meets any applicable regulations.

[6] Entities should apply security best practices to protect planning information such as models, study cases, simulation results, etc.

Operations Planning Applications

Cloud technology in the operations planning horizon centers primarily on the ability to do more in a short time constraint. While not as time constrained as real-time applications, operation planning requires quick, accurate, and trustworthy results to ensure the grid maintains reliable operation. Leveraging cloud computing can not only reduce costs but can likely allow operations planning to explore more thoroughly the impact of potential decisions as well as the impact of many combinations of potential operator actions. Examples where cloud computing may provide benefits include:

- Expansion of available data for use in operational planning analysis
- Increasing the maximum PMU data streams able to feed operational tools
- Running off-line analysis in tandem with real-time analysis for comparison
- Offloading of expensive desktop equipment and setups to support operational tools
- Coordination of planned and maintenance outages
- Capability to perform more detailed and shorter time step simulations (e.g., three phase root-mean-square (RMS) and EMT) for use in operational planning assessments
- Determination with more accuracy any system operating limit (SOL) or interconnection reliability operating limit (IROL)
- Interaction with energy management system (EMS) applications for a wider variety of users and ease of sharing EMS data to a variety of end users (e.g., real-time contingency analysis users)
- Improvement of forecasting fidelity in day ahead time frames
- Calculation of available transfer capabilities (ATCs) through increasingly constrained transmission systems
- Alignment and data quality checks of the model information in the operational tools for matching current day, next day, weekly, and seasonal models as well as alignment in various software platforms
- Customer management systems (CMS) and outage management systems (OMS) interfaces integrated with geographical information systems (GIS) to allow for public to see local outages without overloading operator telephones
- Predictive equipment maintenance and failure predictions of transformers

Real-Time Field Applications

Many of the core reliability and safety functions performed by relays, remote terminal units, sensors, and other devices in a substation rely on very fast actions (microseconds to milliseconds) and require very low latency and very high availability. Devices communicate with the other field devices or with the control center through unidirectional or bidirectional data exchange. However, some devices may store information locally and the data is typically stored within the device itself for a period of time or on another local storage device. This type of data storage configuration is typically used for either: 1) data that is made available for analysis, or 2) very high sampling rates of relatively rare events (e.g., digital fault recorder data). This data can generally be retrieved either locally or remotely, when necessary. Due to the strict operational requirements, making use of regional cloud data center technology may have limited value on its own. However, there are opportunities to utilize cloud-based devices that reside on-premises to support real-time field applications. In these designs, the cloud technology may not be performing the real-time function itself. Hardened, ruggedized, cloud-built industrial internet of things (IIoT) edge devices and on-premises hybrid cloud servers may be viable architectures to complement substations and other distributed or remote sites in support of real-time field applications.

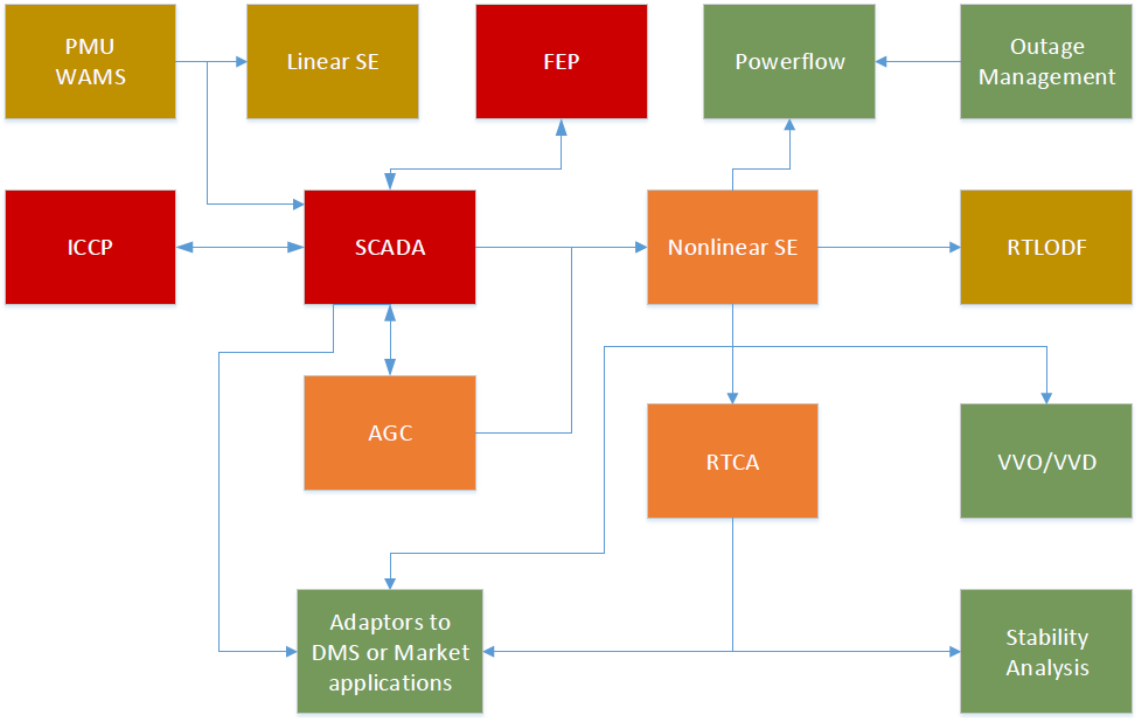
Note that there may be applications that rely on field data that is sent and stored in a central repository (e.g., vegetation management data, drone footage, PMU data, etc.) but the team has categorized this as an off-line application rather than a field application since the data would be used in a centralized location rather than in the field directly.

Real-Time Operations Applications

Real-time operations applications are vital for situational awareness as well as making and implementing well-informed operating decisions. One of the primary benefits of leveraging cloud technology in real-time operation applications includes faster more efficient disaster recovery. The nearly limitless computing resource available in the cloud provides the benefits of superior processing speed. Complex workloads (like transient security assessment calculations) that can take up to 30 minutes to process on-premises are completed in a couple of minutes in the cloud. Unexpected outages of real-time operations applications can leave system operators with impaired visibility. Having previous versions of software stored in the cloud and having production instances running on multiple cloud availability zones or regions allows faster recovery from disasters. For example, suppose an application is deployed in various regions, and one region goes down for some reason. In that case, the traffic can automatically failover to the working regions without any interruptions to the end-users. In other cases where there is a major bug in the software release, a quick rollback can be initiated to restore a previously released, more stable version to minimize impact. The fact that data can be stored in the cloud without capacity constraints also helps with backup and restore purposes. Example workloads in real-time operations applications where cloud technology may provide benefits include:

- Providing a fast scan on system conditions with a shorter cycle for state estimator and/or real-time contingency analysis
- Increasing the number of base cases and operating conditions studied
- Expansion of scenario studies for real-time stability analysis
- Capability to consider more constraints in real-time optimal applications
- Capability to run real-time multiple time-point look-ahead study that assembles the current base case with planning outages and performs thermal/voltage/transient assessment for near future intervals
- Improving efficiency of data exchange between real-time operations applications
- Improving interactions between real-time operations applications and distribution/market applications
- Increasing collaboration between RCs and TOPs. They can view and share information easily and securely across a cloud-based platform.

There may be cloud use cases to be found if historically monolithic applications such as EMS and supervisory control and data acquisition (SCADA) are broken down to their logical service components. The use of microservices and containerization technology create opportunities to develop new architectures hosted in cloud environments for these applications. The typical dependency between main EMS/SCADA applications is illustrated in **Figure 3.1**.



AGC: Automatic Generation Control
DMS: Distribution Management System
FEP: Front End Processor
ICCP: Inter Control Center Protocol
Linear SE: Linear State Estimator
Nonlinear SE: Nonlinear State Estimator
PMU/WAMS: Phasor Measurement Unit/Wide Area Measurement System
RTCA: Real-Time Contingency Analysis
RTLODF: Real-Time Line Outage Distribution Factor
SCADA: Supervisory Control and Data Acquisition
VVD: Volt-Var Dispatch
VVO: Volt-Var Optimization

Figure 3.1: Example Visualization of EMS/SCADA Applications

The real-time operations applications that comprise the EMS/SCADA system (shown in Figure 3.1) can be categorized in the following risk levels.

- **Critical:** FEP, ICCP, and SCADA
- **High:** AGC, Nonlinear SE, and RTCA
- **Medium:** Linear SE, PMU/WAMS, and RTLODF
- **Low:** Adaptors to DMS or Market applications, Outage Management, Power Flow, Stability Analysis, and VVO/VVD

This categorization is based on the following questions intended to help entities evaluate operational restrictions and potential risks of placing real-time applications in the cloud:

- **How is the current real-time application deployed in the EMS and can it be migrated to a cloud solution?** Some applications are more suited for on-premises solutions while others may be migrated to the cloud. Software vendors may even offer cloud-based products today and in the near future, so ensuring the organization fully understands what the migration entails, how it will affect critical business functions, and whether cloud solutions are even an option or priority for applicable vendors will be key. The criticality (i.e., consequences of failure, unavailability, or compromise) of each service or application is key to informing business decisions in this area.
- **What type of cloud deployment models is being used?**

NIST SP 800-145[7] defines four deployment models: private cloud, community cloud, public cloud, and hybrid cloud. Public cloud is provisioned for public use and exists on the CSP's premises whereas private cloud is provisioned for exclusive use by a single organization and may exist on or off premises of the organization. On-premises private cloud options, and/or dedicated connections to a secure cloud environment at the CSP present lower risk for possible real-time applications. Hybrid cloud options may also help ensure security requirements are met while leveraging availability and uptime benefits of cloud-based technology.

- **Is the real-time operation application essential for entities to implement their reliability functions?** Entities use various EMS/SCADA applications based on their reliability functions. For example, AGC and SCADA are critical for Balancing Authorities (BAs) to monitor and control generation output and to calculate area control error. A Transmission Operator (TOP) may use SCADA, SE, and RTCA to monitor and control the transmission network to keep the system in a reliable operating state. FEP and ICCP may be required by both the BA and TOP. Placing non-essential real-time operations applications in the cloud is likely a lower risk than those applications essential to core reliability functions. Some situational awareness tools, advanced monitoring systems, or other tools may be more suitable for initial cloud adoption in real-time.
- **Will the failure of the real-time operation application cause a complete loss of monitoring and/or control capability, and what does the fail-over state look like?** Monitoring[8] and control[9] capabilities are essential for real-time operations. If the failure of the real-time operation application could cause a complete loss of monitoring or control capability, a higher risk should be considered to place this application in the cloud. For example, the loss of SCADA would likely be the most impactful EMS failure. System operators would not have indication of the status of devices or key data points such as MW, MVar, current, voltage, or frequency from RTUs. Furthermore, system operators would not be able to open and close breakers or switches remotely from the control center. Fully understanding the operational impacts for any failure or unavailability of the service is critical. The type of cloud model implemented may impact these considerations.

Security Service Applications

Cloud technology for security service applications centers on the ability to visualize, process, assess, and quickly react to anomalies in a protected environment to mitigate the impact of security events on reliability. Leveraging cloud computing can reduce costs and also allow security operations centers (SOCs) or security teams to assess and analyze potential threat and the impact of a cyber event within their environment more quickly. Examples where cloud computing may provide benefits include:

- Expansion of available data for use in security analysis
- Offloading of desktop equipment and set up to support security tools
- Increased storage capacity to retain security and operational log data for extended timeframes
- Enhanced data analytics and machine learning services that support cyber security incident response and forensic analysis
- Cloud-based single platform tools that increase visibility into IT and OT networks to support situational awareness and threat detection (e.g., next generation antivirus)
- Cloud-based single platform tools that coordinate security maintenance across cloud and on-premises implementations (e.g., patching)

Examples of these types of systems or applications may include the following:

[7] https://csrc.nist.gov/publications/detail/sp/800-145/final

[8] Monitoring capability is the ability to accurately receive relevant information about the BES in real-time and evaluate system conditions using real-time data to assess existing (pre-contingency) and potential (post-contingency) operating conditions to maintain reliability of the BES.

[9] Control capability is the ability to take and/or direct actions to maintain the reliability of the BES in real-time via entity actions or by issuing operating instructions.

- **Electronic Access Control or Monitoring Systems (EACMS):**
  - **Security Information and Event Management (SIEM):**
    - Reduced infrastructure maintenance, enabling more focus on high-value security tasks instead of regular maintenance, monitoring SIEM health, and troubleshooting
    - Increased elasticity to scale the capacity of SIEM compared with capacity-constrained on-premises solutions (e.g., scaling storage for irregular increases in log volume versus losing logs)
    - Advanced analytics and machine learning that allow utilities to mature their security monitoring program through data correlation, behavioral analytics and/or anomaly detection
  - **Next-generation antivirus (NGAV):**
    - Reduce time to identify malware using advanced endpoint protection technologies involving AI and machine learning to identify new malware by examining more elements such as file hashes, URLs, and IP addresses
    - Endpoint security software protects endpoints from being breached including those that are physical or virtual, on- or off-premise, in data centers or in the cloud. It is installed on laptops, desktops, servers, virtual machines, as well as remote endpoints themselves.
    - Administrators can remotely monitor and manage endpoints through a centralized management console that lives in the cloud and connects to devices remotely through an agent on the endpoint.
    - These solutions leverage cloud controls and policies to maximize security performance beyond the traditional perimeter removing silos and expanding administrator reach.
  - **Automated patch management solutions**:
    - Cloud-native automated patch management solutions centralize patching into a single console that can patch hybrid infrastructure and remote environments.
    - IT administrators can set specific rules for new updates including rules for testing new code updates before deployment. This gives IT departments the oversight they need to help with compliance requirements and security maintenance.
- **Physical Access Control System (PACS):**
  - Cloud-based offerings are scalable and allow customers to adapt to the security needs of any number of remote sites, buildings, or doors without limits on controls or logging. They easily integrate with other systems like communications or electronic security systems. The integrations help offer context to physical or cyber monitoring of security standards and employee policies.

Use Cases for Smaller Entities

Cloud technology, particularly when shared across multiple entities at relatively low cost, may provide specific benefits to smaller entities. The cost of standalone products (e.g., SCADA systems, advanced applications, data historians) can be relatively steep for smaller entities, making tools significantly limited. Smaller entities are not able to staff IT and OT resources to properly maintain and secure these systems and applications. Larger entities will often use custom tools, applications, or programs for operational tools whereas smaller entities need off-the-shelf applications. In many cases, information sharing, and shared use of common applications provides tangible benefits for smaller entities. Examples may include:

- **Secure Access to EMS:** Smaller entities may remotely access EMS systems and applications of neighboring TOPs and RCs for situational awareness. In many cases, these entities have read-only privilege for viewing analysis results. The ability to streamline and secure this access across a single platform could provide significant value to these entities.

- **Off-The-Shelf SCADA:** The ability to extend or offer mainstream off-the-shelf SCADA tools to smaller entities (and smaller systems), such as through a joint purchase, could provide additional value for these entities. For small organizations, SCADA solutions are often custom-built or ad-hoc, if they exist at all. Enabling more streamlined off-the-shelf solutions that minimize costs for custom solutions could be beneficial.
- **Customer and Outage Management:** Cloud-based customer management systems and outage management systems with a customer interface and geographic information system integration is another area of focus for smaller entities. This solution could greatly improve customer service during times of customer impact due to outages and overloading of resources (phones, staff, computational power, etc.).
- **Equipment Maintenance and Asset Management – Industry Sharing:** Cloud-based tools that share critical information (e.g., equipment failure data) from a centralized and secure database could streamline asset management and maintenance programs and could enhance reliability through lessons learned and other information sharing.
- **Reliability Study Model Construction:** Software vendors and regional case building entities may be able to host cloud-based tools and products for the effective and efficient development of regional or interconnection-wide planning cases (steady-state, short-circuit, dynamic, etc.). This could help the ease of case creation as well as streamlining case updates and change management.
- **Engineering Drawing Management:** Cloud databases can be used to store engineering drawings, procedures, calculations, and configuration files. These databases can be tied to work order management systems such that relay techs are provided the most up-to-date database files from a master library database (which can be tied back to relay maintenance programs per PRC-005, etc.). Additionally, there are opportunities with collaborative modeling, tuning, and debugging in co-simulations.

Many of these solutions highlight the need for improved accessibility at a minimized cost. They also demonstrate the need to minimize potential errors throughout the planning, design, and real-time operations horizons that are often caused by disparate databases and/or tools rather than leveraging a centralized cloud-based tool. There are likely many more examples of opportunities for smaller entities; however, these provide some concrete examples from NERC engagement with smaller registered entities.

Chapter 4: NERC CIP Compliance Considerations

From a NERC CIP Standards compliance perspective, the most fundamental aspect of cloud technology is understanding what data is being put into the cloud and how that data is being secured. This requires a case-by-case assessment of cloud use cases to determine applicable security controls and how the implementation, and demonstration, of those controls align with the NERC CIP Standards. Once the "what" and the "how" are well understood, then Registered Entities, the Regional Entities, and NERC can delve into understanding how the controls are demonstrated and the role of contractual agreements with the CSP, separation of the underlay and the overlay, and the protections in place between the two layers, etc. A critical consideration for Registered Entities is assuring that sufficient documentation or demonstration in other forms is available both from the entity and the CSP to demonstrate compliance with all applicable requirements.

Cloud service providers architect security differently than traditional on-premises security architectures. These differences may include identity and access management to their underlay environments. For example, some CSP's purposely design their systems to prevent CSP personnel from accessing customer environments and data through strict physical and logical separation controls. These implementations may be supported by logging capabilities that offer customers the ability to see every API call made to and within their environment. Other CSPs may offer specific solutions to control access to a customer environment that offers the entity visibility and requires entity authorization each time CSP personnel needs access. Demonstrating that these controls are in place and meet the NERC CIP requirements necessitates collaboration, agreement, and guidance to be developed by entities, the ERO Enterprise and CSPs. Future compliance demonstration may require consideration of the acceptance of third-party audit records such as SOC reports, or third-party certifications such as FedRAMP as components of compliance demonstration which are typically not necessary in an on-premises environment.

Acceptance of third-party audit reports and third-party certifications is a topic central to enabling cloud adoption. From a compliance assurance and auditing perspective, the Government Auditing Standards (known as the Yellow Book)[10] include requirements pertaining to accepting the work of others. In particular, Section 8.81 states the following:

> ***8.81*** *If auditors use the work of other auditors, they should perform procedures that provide a sufficient basis for using that work. Auditors should obtain evidence concerning the other auditors' qualifications and independence and should determine whether the scope, quality, and timing of the audit work performed by the other auditors can be relied on in the context of the current audit objectives.*

The footnote on section 8.81 references Section 5.80, which states:

> ***5.80*** *Auditors who are using another audit organization's work should request a copy of that organization's most recent peer review report, and the organization should provide this document when it is requested.*

NERC uses these Government Auditing Standards as the foundation of NERC Audits. Further analysis into ways that third-party audit reports and third-party certifications can be used in alignment with this guidance is necessary.

Registered entities adopting cloud technology will also need to consider the security controls available to prevent unauthorized access to their overlay environment, and how to demonstrate that they are implemented. Those controls may include, but are not limited to, encrypting the cloud overlay environment, managing access to the encryption keys, implementing, and managing identity and access management controls that include authorization,

[10] Government Auditing Standards, 2018 Revision. Technical Update April 2021: https://www.gao.gov/assets/720/713761.pdf

development and use of discrete access roles, and log collection and retention. Some of these controls are likely to require additional and / or different audit evidence than an entity has needed to produce for on-premises environments.

An example of where these parties have come together in support of cloud adoption successfully is the NERC published *ERO Enterprise CMEP Practice Guide: BES Cyber System Information*.[11] The Practice Guide opened the door for Registered Entities to move BCSI data into the cloud, breaking down the tie to specific physical assets and data repositories, and included guidance that NERC Regional Auditors should consider access to include any instance or event during which a user obtains and uses BCSI. This clarity enabled utilities wanting to use third-parties such as CSPs to understand the controls necessary to implement a secure and compliant program. This also led to the formation of Project 2019-02 to revise the NERC CIP Standards, which will provide clearer guidance for allowing Registered Entities to utilize cloud technology for sensitive data storage.

Beyond CIP-004 and CIP-011 challenges, there are additional obstacles with other NERC CIP standards that would need to be addressed once access requirements between the overlay and underlay are addressed. These include, but are not limited to, the following:

- CIP-005 utilization of External Routable Connectivity
- CIP-006 how cloud-based PACs are deployed, logged and monitored
- CIP-007 logging of events and how event log reviews occur

These issues will need to be addressed by stakeholders including industry, NERC and registered entities working collaboratively through future standards revisions, development of compliance guidance and other mechanisms. Given the expected timetables for CIP standards revision and development of this magnitude, however, it may serve industry well to make additional efforts towards cloud adoption that build consensus on a more optimistic timeline.

[11] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20_%20BCSI%20-%20v0.2%20CLEAN.pdf

Chapter 5: Recommended Industry Actions Moving Forward

The following are recommended actions that NERC and its stakeholders should take to remove barriers of adoption and enable innovation and exploration of secure and reliable use of BES operations within CSP hosted clouds:

Long Term:

- **Recommendation L1:** SITES recommends industry evaluate the potential justification for additional SARs related to cloud security in the context of the findings identified in this white paper and other ongoing industry cloud-computing activities.

Short Term:

- **Recommendation S1:** SITES recommends industry perform NERC CIP audit tabletops covering CSP cloud-hosted BES cyber system use cases to identify compliance and security risks in order to continue building knowledge for industry and subsequently informing the development of CMEP Practice Guides when assessing registered entities in similar audit scenarios.
  - Intended to identify further problems to be solved including needs to modify evidence request tools, RSAWs, and specific security, compliance, implementation, CMEP guidelines, etc.
- **Recommendation S2:** SITES recommends NERC and the Regional Entities consider how to review and accept (as reasonable assurance of compliance) the following sources if provided as evidence of compliance with applicable Reliability Standards: accredited third party auditors providing cloud-based security framework certification for CSPs and independent cloud risk assessments of CSPs performed by registered entities. The intention is for NERC and the Regional Entities to consider relying on these measures as evidence for the security of a CSP underlay environment in an assessment of a registered entity utilizing BCS in a CSP cloud. SITES recommends NERC and the Regional Entities further consider the following:
  - Where a SaaS provider utilizes a separate IaaS provider, the SaaS provider would use third-party audit evidence provided by CSP/IaaS provider for the security of the underlay, and documentation/third-party audit evidence for the security of the overlay they are providing to the registered entity.
  - The registered entity would then be responsible for evidencing security objectives for the overlay and/or underlay depending upon the shared responsibility model.
- **Recommendation S3:** SITES recommends industry endeavor to map NERC CIP standards and requirements equitably to prominent cloud-based security control frameworks, providing a foundation for the potential use of accredited third-party auditor reports and certification of CSP products and services to be utilized as accepted work of others by ERO Enterprise auditors within audits of registered entities as part of a shared responsibility model between the CSP and registered entity for BES cyber system hosted in the cloud. E.g. ISO/IEC 27017
- **Recommendation S4:** SITES recommends vendors with cloud-based products and services for the electric sector take a pro-active approach to seek accredited third-party certification to cloud-based security frameworks which encompass the NERC CIP requirements, and to furnish both audit reports associated to such certifications, and CIP implementation guidance or controls documentation for their cloud products.
  - SITES recommends cloud security frameworks where consensus on equitable mapping to NERC CIP is building, such as with FedRAMP Moderate.
- **Recommendation S5:** SITES recommends the ERO Enterprise develop compliance implementation guidance for registered entities to evidence control ownership within a shared responsibility model for their cloud-hosted BES cyber system.

- **Recommendation S6:** SITES recommends industry develop and standardize use of a CIP-tailored cloud risk assessment framework for independent use by registered entities during evaluation and selection of CSPs for cloud hosted BES cyber system. The risk assessment framework should likewise be tied to a standardized cloud security framework (e.g., Cloud Security Alliance's Cloud Controls Matrix). Furthermore, CSPs may limit their participation in the risk assessments by pro-actively furnishing the necessary input to the risk assessment through controls implementation and management documentation. SITES recognizes that smaller CSPs and SaaS vendors may find the process for third-party certification too substantial or costly, potentially creating a gap that may be filled by independent cloud risk assessments performed by registered entities.

Appendix A: A Look at EMS Cloud Deployment

Table A.1 illustrates a deconstructed view of the elements of an EMS and the top two business drivers for possible adoption of cloud technology. For each element of the EMS, the frequency execution and the required roundtrip execution time are also specified (for a general understanding of operational requirements). Next, each element is assigned a risk factor, in particular the overall response time of each application as well as its criticality to real-time operations are defined. High risk applications are defined here as those applications that the operators rely heavily upon that if rendered unavailable could have a significantly adverse impact to BPS reliability in a short period of time. With these two indicators, the team determined which elements could possibly be moved to the cloud and whether that would be a local, hybrid or full cloud implementation. This table is intended as a high-level illustration for entities to consider based on their own risk tolerance.

Table A.1: Deconstructing EMS for Cloud Evaluation

Deconstructed View of the Solution Area	Top Two Business Drivers				Frequency of Execution	Required Roundtrip Execution Time[12]	High Risk Application[13]	Cloud vs. Hybrid vs. Local
	Agility/CTI	Cost Savings	Resilience	Scalability				
Front End Processor					millisecond	millisecond	Yes	Local
SCADA					millisecond	1 second	Yes	Local
ICCP					millisecond	millisecond	Yes	Local
Automatic Generation Control (AGC)					2 seconds	< 1 second	Yes	Local
Nonlinear State Estimation (SE)					1 to 5 minutes	< 30 seconds	Yes	Hybrid
Real-Time Contingency Analysis (RTCA)					1 to 5 minutes	< 60 seconds	Yes	Hybrid
RTLODF (Real-Time Line Outage Distribution Factor)			Y	Y	1 to 5 minutes	< 5 seconds	No	Cloud
Adapters to DMS or Market applications			Y	Y	1 to 5 minutes	< 5 seconds	No	Cloud
Outage Management			Y	Y	By request	< 5 seconds	No	Cloud
Power flow			Y	Y	By request	< 10 seconds	No	Cloud
Stability Analysis (voltage and transient)		Y		Y	5 minutes for voltage 15 minutes for transient	< 5 minutes for voltage < 15 minutes for transient	No	Cloud

[12] This is the roundtrip time for the application to execute completely including data input, computation, and results output, with all delays and communications.

[13] High risk applications are defined here as those applications that the operators rely heavily upon that if rendered unavailable could have a significantly adverse impact to BPS reliability in a short period of time.

Table A.1: Deconstructing EMS for Cloud Evaluation

Deconstructed View of the Solution Area	Top Two Business Drivers				Frequency of Execution	Required Roundtrip Execution Time[12]	High Risk Application[13]	Cloud vs. Hybrid vs. Local
	Agility/CTI	Cost Savings	Resilience	Scalability				
Volt-VAR Optimization/Dispatch		Y		Y	10 minutes	< 5 minutes	No	Cloud
Dashboard Visualization						<1 second		
Linear SE			Y	Y	60 seconds	< 10 seconds	No	Cloud
PMU/Wide Area Monitoring System (WAMS)			Y	Y	5 seconds	< 1 second		Cloud

Key Takeaways of Table Exercise

The table above shows that once an EMS is deconstructed, its functions do not all have the same critical requirements of speed/performance and nor do they share the same risk. Traditionally an EMS is a monolithic application responsible for executing all functions. The performance requirements and risk of an EMS as a monolithic application comes from its most demanding functions such as SCADA, AGC and ICCP, etc. However, if an EMS was designed and built as a collection of microservices where each EMS function was represented by its own highly scalable microservice then a utility can decide where each function runs based on its individual risk and speed/performance requirement. This approach opens the door to the use of virtualization, containers, distributed processing, and cloud technology without putting to risk critical operations. Figure A.1 shows an example of a potential EMS application architecture between a CSP cloud environment and on-premises.

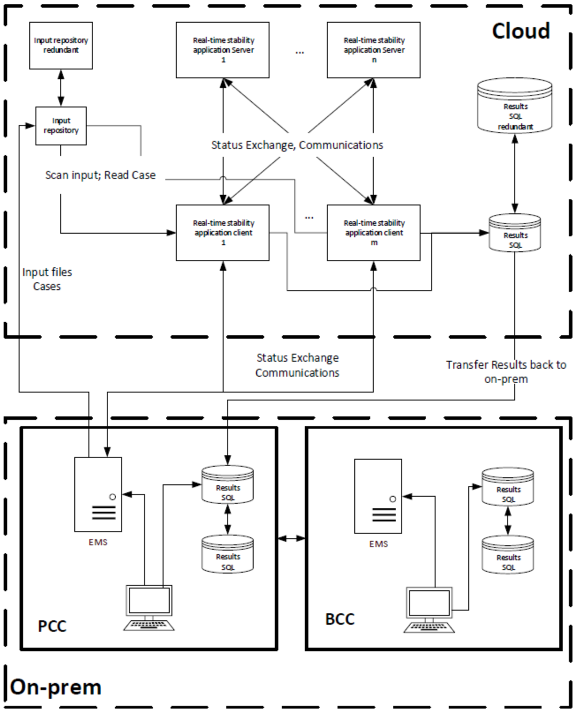

Cloud
Input repository redundant
Real-time stability application Server 1
...
Real-time stability application Server n
Input repository
Status Exchange, Communications
Results SQL redundant
Scan input; Read Case
Real-time stability application client 1
...
Real-time stability application client m
Results SQL
Input files Cases
Status Exchange Communications
Transfer Results back to on-prem
EMS
Results SQL
Results SQL
PCC
EMS
Results SQL
Results SQL
BCC
On-prem

Figure A.1: System Architecture for Cloud Technology for Stability Study Applications

Appendix B: Explanation of BROS and CIP-002-5.1a

The scope of the CIP Cyber Security Reliability Standards is restricted to BES cyber systems that would impact the reliable operation of the BES. In order to identify BES cyber systems, Responsible Entities determine whether the BES cyber systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the initial scope for consideration includes only those BES cyber systems and their associated BES cyber assets that perform or support the reliable operation of the BES. The definition of BES cyber asset provides the basis for this scoping.

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES cyber systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES." Responsibility for the reliable operation of the BES is spread across all Regional Entity registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES cyber systems that would be in scope. Responsible Entities use Table B.1 from CIP-002-5.1a to determine applicable BES reliability operations services (BROS) according to their Function Registration type.

Table B.1: Entity Registration and the BROS

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Appendix C: References

This document is not intended to serve as a detailed and technical reference for cloud technology; rather, it is intended to provide guidance and considerations for industry adopting cloud technology moving forward in a secure and reliable manner. A key goal of this document is to help bridge the gap between engineering and security considerations, and better integrate these concepts holistically. The following are links to reference documents that provide more detailed information related to the concepts described in this document:

- *NERC Security Guideline for the Electricity Sector - Supply Chain Risks Related to Cloud Service Providers*

  https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cloud_Computing.pdf

- *NERC Security Guideline for Electricity Sector Primer for Cloud Solutions and Encrypting BCSI*

  https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline_BCSI_Cloud_Encryption.pdf

- NATF Energy Sector Supply Chain Risk Questionnaire:

  https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

- AWS *The Utility Executive's Guide to Cloud Security*

  https://d2908q01vomqb2.cloudfront.net/c5b76da3e608d34edb07244cd9b875ee86906328/2020/08/10/AWS-Utility-Executive-Guide-to-Cloud-Security-1.pdf

- AWS *Power & Utility Path to Production in the Cloud*

  https://d2908q01vomqb2.cloudfront.net/c5b76da3e608d34edb07244cd9b875ee86906328/2021/01/04/AWS-Power-and-Utility-Path-to-Production-in-the-Cloud-1.pdf

- IEEE Report on Practical Adoption of Cloud Computing in Power Systems

  https://resourcecenter.ieee-pes.org/publications/technical-reports/PES_TP_TR92_AMPS_012822.html

- NATF Supply Chain Security Assessment Model

  https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

- MITRE ATT&CK® Matrix for cloud-based techniques, and industrial control systems (ICS)

  https://attack.mitre.org/matrices/enterprise/cloud/

  https://attack.mitre.org/matrices/ics/

Appendix D: Contributors

Contributors to this whitepaper include members of NERC, the Regional Entities, SITES, and other industry stakeholders. Contributions include research, discussion, writing, and editing. A special thank you goes to AWS staff for their significant collaborative efforts and contributions to this whitepaper. In alphabetical order, the list of contributors include the following individuals:

Table D.1: Whitepaper Contributors

Name	Name	Name	Name
Abhineet Parchure	David Hartley	Karl Perman	Ryan Carlson
Alejandro Gonzalez	David Metheny	Katherine Street	Ryan Quint
Andrea Koch	Doug Peterchuck	Kristine Martz	Sean Crimmins
Anthony Pearce	Eric Carriere	Larry Collier	Scott Pelfrey
Ashwini Paranjape	Eric Chen	Maggy Powell	Sean Randles
Barry Jones	Ian King	Manu Parashar	Song Zhang
Barry Kuehnle	James Ball	Marc Child	Stan Hoptroff
Benny Naas	Jay Cribb	Marisa Hecht	Stephanie Lawrence
Brenda Davis	Jay Moser	Michael Cloud	Steven Dougherty
Brent Sessions	Jeffrey Sykes	Michael Sanders	Suzanne Black
Brian Hogue	Jeremiah Miller	Mike Unum	Thomas Peterson
Casey Werth	Jerrod Montoya	Morgan King	Thomas Standifur
Chris Holmquest	Jerry Reed	Muralidhar Cheruvu	Tom Hofstetter
Curtis Dorcheus	John Biasi	Philippe Comperon	Tracey Stewart
Dan Goodlett	John Lemmon	Pierre Janse van Rensburg	Wally Magda
Dan Goyne	John Porter	Ranjan Banerji	Wei Qiu
Dan Grundman	Joseph Baugh	Ravi Pradhan	Xiaochuan Luo
Danny Johnson	Joseph Januszewski	Roger Hales	Xing Wang
Dave Sopata	Joyce Harris	Ron Ross	Zach Trublood