aws power and utilities

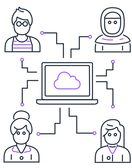
# Power & Utility Path to Production *in* the Cloud

**Using the AWS Cloud for Regulated Workloads**

Once you have an understanding of the business drivers moving you to the cloud, it's time to look at how you can use AWS services to become more secure and resilient. Get your organization ready, engage with AWS, and work together on the path to the AWS Cloud.

## 1. Identify and Engage Stakeholders:

Early engagement with your Security, Risk and Compliance teams is important for an effective path to production. Often, these teams are separate from other teams responsible for cloud delivery and they have different perspectives. Helping them work together to achieve the overall business outcome is a key part of successful cloud deployment. Keep in mind operational technology (OT) decision makers may differ than information technology (IT) decision makers and have different considerations and requirements driven by compliance and operations.



## 2. Build Capabilities and Knowledge:

We strongly encourage you to create a **Cloud Center of Excellence (CCoE)** composed of a cross-functional team with diverse skills and backgrounds to drive transformation. Take advantage of **training opportunities** for CCoE team members to familiarize themselves with the **AWS shared responsibility model** and the AWS services that can make it easier to achieve your objectives. The **AWS Cloud Adoption Framework – Security Perspective** helps customers get started across four main components of the framework: Directive, Preventive, Detective, and Responsive controls. The **AWS Well-Architected Framework** describes the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. The five pillars of operational excellence, security, reliability, performance efficiency, and cost optimization provide a consistent approach for the CCoE team to evaluate architectures, and implement designs that can scale over time.

## 3. Consider Operational Requirements:

Operational requirements can vary across workloads whether for generation, transmission, distribution, or behind-the-meter. The decision to adopt cloud solutions for these systems includes consideration of reliability, latency and the criticality of the operation. Although many operating services are ripe for cloud computing, some critical functions may remain out of scope for cloud due to low latency requirements. However, AWS-provided edge technologies such as **AWS Outposts**, **AWS IoT Greengrass**, **AWS Snow Family** and **AWS IoT Core** devices can help meet these requirements. Frameworks like the Purdue Enterprise Reference Architecture (PERA) for industrial control systems or other frameworks can help you map workloads by operational needs.

## 4. Understand Regulatory Requirements:

Power & Utility workloads may be subject to applicable regulatory requirements, such as NERC CIP or 10CFR810 in North America, Network and Information Systems Directive (NIS-D) in the European Union, or PCI requirements for online billing data. Mapping regulatory obligations to common controls and establishing mechanisms to demonstrate compliance are critical steps in adopting cloud services. You should also consider a compliance assessment prior to production, for example, a documentation and evidence review.

## 5. Establish Internal Security Principles:

Understand your security requirements and how cloud maps to those requirements. Frameworks such as the NIST Cybersecurity Framework provide a general view of security control objectives for your organization. The **AWS Well Architected Framework** provides guidance for building and operating securely in the cloud.

## 6. Understand Security of the Cloud:

We encourage a wide range of stakeholders within your company to understand the **shared responsibility model** and the way AWS demonstrates its security of the cloud through compliance to multiple security assurance programs. Your teams can access and review AWS security assurance reports, such as our System and Organization Controls (SOC) reports, available on **AWS Artifact.** Through mechanisms such as an annual vendor risk management process, you can track your vendor risk assessments. We encourage you to engage with your local AWS team to understand the security controls in place specific to the AWS services you adopt, and to discuss how your requirements and compliance needs can be met.

## 7. Embrace Security in the Cloud:

You can use AWS services to automate security processes, improve visibility of your security and control environment, and enable near-real time continuous compliance across domains such as identity, logging and monitoring, data protection, and incident response. We encourage you to develop, review, and approve applications, data, and resiliency classification processes, as well as cloud security standards and policies. You can build granularity into your security control management processes and data access capabilities, establish a process for reviewing AWS services and approving them for internal use, as well as an approval process for moving regulated, confidential, or personally identifiable information (PII) data to the AWS cloud. Security immersion days, training (e.g., **AWS Security Fundamentals, AWS Security Engineering**), and certifications (e.g., **AWS Certified Security – Specialty**) are resources to support your efforts.

## 8. Verify Procurement Agreements:

Legal, procurement, and outsourcing teams within your company can also familiarize themselves with the **AWS shared responsibility model** and cloud services, as using the cloud can be different from the ways that companies like yours traditionally procure and consume hardware and software. You may also need to verify that the appropriate agreements are in place prior to production to fulfill corporate or regulatory requirements. For example, in North America, agreements with cloud service providers may be part of a company's compliance evidence.

## 9. Build Cloud Architecture:

Once you have identified your security control requirements (per items 3-5 above), you can then build them into automated, scalable architectures. **AWS Control Tower**, **automatic provisioning**, **continuous compliance**, and **AWS Well-Architected Framework** are important components of this build phase. Work with AWS specialists to define the architecture that meets your needs. AWS has quick starts and deployment guides that can help for example **to support NCSC and CIS for UK Official workloads**.

## 10. Establish Internal Assessment Routine and Cloud Governance:

Defining organizational roles and governance are valuable to implementing and sustaining security and AWS services can be used to automate and streamline governance activities. You can use the **three lines of defense model** to establish a governing body, control owners, risk management teams, and audit functions to perform assessments. These assessment activities can include security assessments of your platform and workloads, review of your cloud security strategy with internal or external audit functions, and penetration testing of your resources. **AWS Audit Manager** and **AWS Conformance Pack** templates provide you with a compliance framework for you to create security, operational or cost-optimization governance checks. Before deploying production workloads, you may need to design and/or go through a production sign-off, operational readiness, or permit process. Once in production, governance can include routine assessments of the environment in use.

## 11. Prepare Compliance Program and Audit Planning:

Depending on the jurisdiction, you may have regulatory requirements to fulfill before using cloud services for regulated workloads, such as regulatory approval prior to going live, or security controls subject to regulatory audits. We encourage you to build and test your regulatory compliance documentation with a mock audit or third party assessment to increase your compliance assurance before regulatory review.

AWS security and compliance experts help customers with answers about AWS's security and control environments and with guidance on AWS's cloud security best practices. Visit the **AWS Power & Utilities security page** for more.

**Deploy, Test, & Run Workloads in the Cloud!**

aws power and utilities