Securing Water Utilities with AWS

First published March 27, 2023

A research collaboration with

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract and introduction

Abstract

Today, many U.S. water utilities want to implement cloud-based information technology (IT) and operational technology (OT) solutions to realize the operational and security benefits of the cloud. This whitepaper discusses the business drivers associated with cloud adoption in the U.S. Water Sector, cyber security trends, and outlines best practices for implementing cyber security controls at a water utility.

This whitepaper was written in conjunction with Bluefield Research, an independent insight firm focused exclusively on water markets. It includes recommendations, lessons learned, and insights from thought leaders and industry when considering cloud technology. It builds on those insights and offers ways that AWS and AWS partners can help water utilities of all sizes meet many of their cyber security challenges using familiar cyber security concepts and frameworks like the NIST CSF.

Are you Well-Architected?

The AWS Well-Architected Framework helps you understand the pros and cons of the decisions you make when building systems in the cloud. The six pillars of the Framework allow you to learn architectural best practices for designing and operating reliable, secure, efficient, cost-effective, and sustainable systems. Using the AWS Well-Architected Tool, available at no charge in the AWS Management Console, you can review your workloads against these best practices by answering a set of questions for each pillar.

For more expert guidance and best practices for your cloud architecture—reference architecture deployments, diagrams, and whitepapers—refer to the AWS Architecture Center.

Introduction

While the U.S. water sector's awareness of both cyber security and cloud computing have grown significantly in the past few years, many water utilities are challenged with where to start when it comes to adopting cloud solutions. More than deciding what to adopt, leaders are tasked with understanding and mitigating the cyber risk associated with the technology they use. Since 2021, there has been a significant U.S. Government

focus on developing and offering guidance on cyber security controls to protect critical infrastructure due, in part, to an increasing prevalence of reported cyber events.

If you are a water utility leader considering investing in AWS or AWS partner technology, keep reading to learn about cyber security guidance provided by the U.S. Government, AWS, and other leading industry organizations. You'll also see AWS resources that can help you implement security controls while building on AWS or AWS Partner solutions.

Cyber security and the United States Water Sector

The U.S. Water Sector plays a key role in supporting public health and the environment. Like many critical infrastructure sectors, drinking water and wastewater treatment organizations are responsible for understanding the risk profile of the industry and implement appropriate controls to mitigate risk. While cyber security is a complex subject, there are many ways that technology can help support critical infrastructure organizations in reducing risk.

While cyber security events such as the compromise of a U.S. water treatment facility in February, 2021 are publicized, many informational technology (IT) and operational technology (OT) cyber risks can be addressed through consistent good security hygiene. A thoughtful cyber security approach can benefit an organization's security posture in the context of a variety of common risk scenarios.

According to the Cyber security and Infrastructure Agency (CISA), the United States Environmental Protection Agency (US EPA), and the National Security Agency (NSA), U.S. water and wastewater utilities are working to manage the following risk scenarios: spear phishing to deploy malware such as ransomware, insider threats from current or former employees who maintain improperly active credentials, exploitation of unsupported or outdated operating systems and software, and exploitation of control system devices with vulnerable firmware versions. Today, there are technologies and tools available to utilities to help manage these risks through increased visibility, automation, and monitoring.

Improving cyber resilience across the U.S. water sector, and globally, requires technology and innovation. Technologies, like the AWS cloud and AWS Partner solutions, that can be managed by third parties, that are inexpensive, and can keep pace with the ever-changing threat landscape. A critical component of new technology adoption is understanding the security of those tools, and how they fit into your security governance program. In the U.S., the Water Sector has relied on voluntary cyber security guidance and frameworks, but it can be difficult to prioritize IT and OT cybersecurity practices that meaningfully reduce the likelihood and impact of known risks and adversary techniques.

United States Government focus on Critical Infrastructure

The water industry presents an interesting challenge to the cyber security community due to the localized, fragmented nature of the sector. In many geographies around the world, including the U.S., water utilities are not centralized with many of them serving fewer than 5,000 people. These small utilities often struggle with funding, staffing and technology adoption.

In 2022, the United States Government focused on a series of initiatives and goals aimed at improving the cyber security of critical infrastructure sectors. U.S. Government Agencies including the Cybersecurity and Infrastructure Security Agency (CISA) plan to continue these initiatives. In 2023, CISA plans to concentrate more attention on sectors that are targeted by adversaries because of the essential services they provide but who may not have the resources to defend themselves, including the Water sector.

CISA released voluntary Cross-Sector Baseline Cybersecurity Performance Goals (CPGs) to help establish a common set of fundamental cybersecurity practices for critical infrastructure, and help small and medium-sized organizations kickstart their cybersecurity efforts. The CPGs are not just another set of controls, but are meant to supplement the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), which is often used as guidance in the U.S. Water Sector. One key benefit of this approach is that the CPGs are intended to help critical infrastructure operators prioritize their security practices across their IT and OT environments.

The role of cloud computing in the Water Sector

Water Utilities, like most other utilities and corporations, are realizing the benefits of cloud technology. In addition to unlocking historically siloed data, water utilities are realizing that the total cost of ownership for IT operations are reduced by working in cloud environments. Leading this change in thinking are market forces impacting the supply chain for water utilities.

In the past two years we have seen industry leaders such as Xylem, Innovyze, Neptune and Badger innovating using cloud technology like AWS, and delivering Software-as-a-Service (SAAS) solutions. Bluefield projects that global-spending on cloud-based software in the Water sector will scale at a 12.7% compound annual growth rate (CAGR) between 2021 and 2030, in comparison to 5.2% for on-premises software, reinforcing the importance of cloud security for water utilities.

In addition, cloud technology has enabled rapid expansion in innovative startups for the sector. Companies like BlueConduit, Aquasight and Qatium are built natively on AWS and allow for very quick deployment and updating to solve critical water challenges.

Figure 1 below depicts the barriers to cloud adoption in utilities. Cloud security concerns were identified as the most significant barriers to cloud adoption over the past several years.

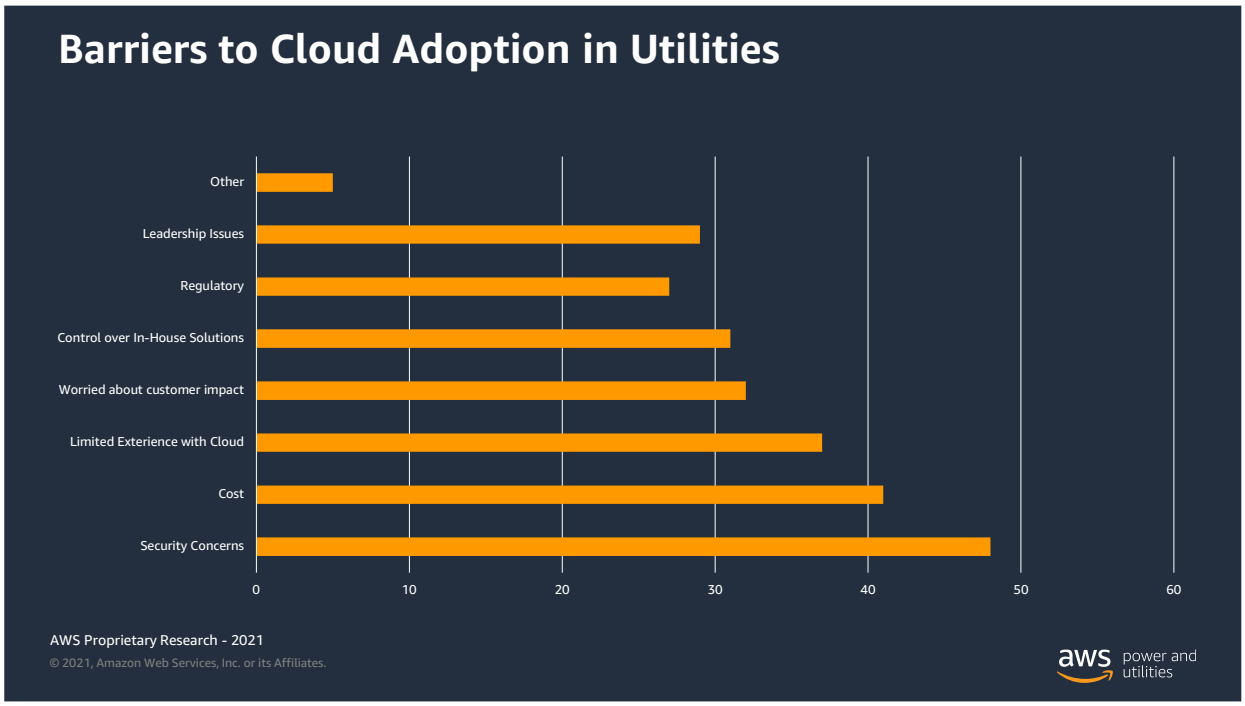

Figure 1 - Barriers to Cloud Adoption in Utilities

However, this paper begs the question: “Will this barrier quickly turn to the largest driver of cloud adoption?” Given where global regulatory bodies are headed with cyber security requirements; one can see how this concern will turn into an enabler of cloud adoption as water utilities need to demonstrate better control of their systems and assets.

Mapping points of opportunity: Areas for cloud adoption enhancements

Water utilities can significantly improve their security posture through the implementation of technical controls. For example, cyber risk is significantly reduced when customers fully embrace multi-factor authentication (MFA). Multi-factor authentication (MFA) for AWS Identity and Access Management (IAM) is a best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to a device, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources. As most people with smartphones understand today, cloud technologies and services are simple to build with MFA security.

Cloud technology for OT & SCADA

Unlike the above IT issues that focus on managing and processing data, operational technology (OT) includes Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, among others that are

WATERS EDGE

Edge computing is simply the processing of data closer to the data source—instead of relying on cloud technology or a centralized data center to do the computing. Edge devices for water utilities can include smart meters, pressure and water quality sensors, and flow measurement devices. These devices can now compute data locally and provide a more efficient means of transmitting and processing water or customer data.

This can be very helpful to utilities that may soon have thousands of IoT devices on a single network. If all of those IoT devices were to try to transmit data individually to the cloud environment or data center, it would require a lot of bandwidth and increase latency. Thus, the use of edge devices provides a valuable cost savings mechanism for these types of organizations.

However, edge devices may pose additional cybersecurity risks that are not present in more analog devices. Cloud technology helps manage and provision these edge IoT devices in a way that helps make these devices much more secure than with on-premises systems. For example, AWS services like IoT Core for Lorawan become increasingly useful to water utilities ingesting data over Lora like services.

used to support real-time operations. The OT pillar covers everything from controls, safety and instrumentation functions such as water treatment plant operations, chemical dosing and energy management.

It has historically been a challenge for water utilities to embrace Cloud-based systems primarily due to cyber security concerns and the availability of technologies that integrate data from IT and OT systems. However, as cloud technologies advance, and IT and OT technologies continue to converge, use of cloud technology for OT systems will need to be considered.

Water utilities and vendors are showing increasing interest in cloud integration for a variety of reasons, including the desire to increase competitive edge, boost reliability, provide flexibility, enable advanced analytics, and support automation. Operating in a cloud environment also allows utilities to better focus on predictive maintenance, redundancy, backup, recovery, and, ultimately, operational excellence. For critical infrastructure, like water, this is essential as disruptions can have large public health, environmental and economic impacts.

However, it is important that water utilities understand the full ramifications of OT cloud migration and have strong partners in these areas. For example, the Idaho National Laboratory (INL) has been working on the concept of Consequence Driven Cyber-Informed Engineering (CCE). West Yost, whose industry leadership comments are highlighted below, is working with INL to bring CCE to the water market. Having a broad view and knowledgeable partner in your cloud OT journey can be at a minimum helpful and more likely critical.

Insights & takeaways from industry experts

While the water sector's awareness of both cyber security and cloud computing have grown significantly in the past few years, many industry experts have been thinking about these issues and trends for much longer. In order to capture these thought leaders' insights, recommendations, and lessons learned, we spoke with more than 25 industry stakeholders representing 12 prominent organizations, including utilities (e.g., Houston Water, Seattle Public Utilities), technology companies (e.g., Xylem, Innovyze), and industry associations and consultancies (e.g., American Water Works Association, Moonshot Missions).

Here's what they had to say:

Utility Professionals:

1. **Now is the time for cloud adoption.** Utility professionals cited a wide range of reasons for migrating select systems and data to the cloud. Some emphasized the unique ability of cloud-based systems to manage, integrate, and analyze massive amounts of data, particularly as utilities increasingly invest in smart metering networks and real-time network monitoring systems. Others talked about the product lifecycles of applications that they rely on, noting that many legacy on-premises systems are no longer supported or lack the modern functionality of cloud-hosted Software-as-a-Service (SaaS) alternatives.

   Potential cost and labor savings of cloud systems were also crucial considerations for several utility stakeholders. Brad Hoglund, Director of Enterprise Application at the Boston Water & Sewer Commission (BWSC), mentioned that as a large utility with a relatively small technology team, he and his staff "have to figure out a way to trim some of the overhead" associated with managing their complex IT infrastructure, and they "can abate some of that overhead with a cloud or hybrid approach." Similarly, Sarah Braman, Senior Water Resources Engineer at the Town of Cary, North Carolina, said that the attraction of cloud-based systems was that her organization "could get ongoing support and help mitigate the internal maintenance requirements."

   Though most of these utility stakeholders acknowledged that they are still in the early stages of cloud migration, with just a few of their core software systems and databases hosted in the cloud to date, they stressed the urgency of getting comfortable with cloud computing sooner rather than later.

   According to Satish Tripathi, P.E., Managing Engineer for Water Infrastructure Planning at Houston Water:

   "We need to come out and adopt these technologies. Without trying it, we will not see whether it is secure or not. The cloud is definitely our future world, and the earlier you test it, the more experienced you will be. Utilities shouldn't just wait around to see what others will do – if everyone takes that position, then who will jump into the water first?"

2. **The cloud is not a silver bullet – utilities still need to do the work to maintain security.** While the utility professionals we spoke with recognized the clear operational and financial benefits of cloud-based systems, they also raised some important concerns related to security in the cloud, particularly for control systems like SCADA.

Evan Fernandes, Director of IT Security at BWSC, observed that even though cloud services providers "have resources to take care of security, with big teams managing and monitoring their systems," utilities still share the responsibility for maintaining network security in collaboration with their technology partners. His BWSC colleague, Director of IT Infrastructure Matthew Gabrick, agreed, noting that in the event of a breach, "the reputation damage will lie with you rather than the cloud provider at the end of the day."

A significant challenge highlighted by several utility IT experts is the lack of technical capacity and experience in the water industry at large, particularly when it comes to cyber security and cloud technology. This challenge is especially acute for small and mid-sized utilities facing budgetary and staffing constraints, but it can be an issue for larger, better resourced organizations as well.

According to Dylan Morris, Cybersecurity Risk Manager with the City of Seattle: "We have a very large IT infrastructure team that does on-prem infrastructure – it's what they know, what they've done for the past 30 years. So transitioning that team, that in-house knowledge, to the cloud is difficult. That kind of pivot takes resources and a different strategy."

3. **Cyber security is a state of mind.** The utility experts we spoke with agreed on the importance of developing a culture of cyber security at the organizational level, regardless of whether utility systems and data are hosted locally or in the cloud.

Steve Lavender, Strategic Technology Advisor at Seattle Public Utilities, drew a parallel between cyber security and occupational safety, noting that staff members are most vulnerable in either case when they are distracted by the task at hand and not thinking about safety or security. His colleague, Dylan Morris, agreed, likening good cyber security practices to a "muscle" that must be exercised regularly by staff at all levels of the organization.

So, what can utility managers and IT professionals do to encourage their colleagues to exercise this muscle on a regular basis? Utility experts cited several inventive practices, including:

- Provide regular, jargon-free communication to utility staff about cyber security threats and consequences.
- Play to people's competitive side – make it a contest between departments to complete cyber security training programs first or perform the best in phishing tests, and offer a prize (free lunch, extra vacation time, etc.) to the winners.

- Make staff feel personal responsibility for their cyber security practices by requiring employees to sign cyber security accountability agreements as part of onboarding.
- Use a combination of carrots and sticks – while it is important to convey the individual and organizational consequences for poor cyber hygiene, it is equally important to empower teams to make good decisions, maintain open lines of communication, and make cyber security training fun and engaging.
- Make sure that upper management is bought in and understands the importance of cyber security so that they can lead by example from outside the IT or security department.

Though these practices can all help to build a culture and mentality of cyber security across an organization, utility experts stressed that cyber risk must be continuously managed. Several of the IT and cyber security professionals that we spoke with emphasized the importance of assuming – and preparing for – the worst-case scenario rather than counting on the best-case scenario. As Evan Fernandes from BWSC noted:

“Unfortunately, people that haven’t been compromised before often take it lightly; they think they’re not at risk. Everyone thinks that a cyberattack won’t happen to them, it will happen to someone else. But it can happen to anyone – even if you do everything right.”

Industry Experts:

1. **Cloud computing is a trusted, proven solution for organizations around the world.** Stakeholders from technology companies, consultancies, and industry associations explained the cyber security advantages of cloud technology from the perspective of both the water utility sector and their own businesses.

   As Rick Gruenhagen, Chief Technology Officer at Innovyze, put it: “from our perspective, the security of cloud-based systems is something that’s a solved problem – solved, because we have so many other industries building services in the cloud,” such as the financial and healthcare sectors. Companies in these industries often face much stricter regulations governing the secure collection, storage, and use of customer data than do water utilities, and cloud services providers like AWS have developed their own cyber security practices and solutions to help customers meet these standards.

Other industry experts highlighted the vast resources and cyber security expertise of technology companies like AWS, particularly when compared with small and mid-sized utility organizations.

> According to Mahesh Lunani, Founder and CEO of Aquasight, "there is no way that any utility in the world can even remotely afford the cyber security experts that AWS can afford – forget utilities, even some of the Fortune 500 companies cannot afford that."

While utilities still share responsibility for their security with their technology partners, leveraging the IT and cyber security infrastructure of cloud specialists enables utilities to focus more of their own time, energy, and resources on doing what they do best – namely, delivering high-quality water, wastewater, and stormwater services for their customers and communities. George Hawkins, Founder and President of Moonshot Missions, drove home this point with a powerful analogy:

> "It doesn't make sense to have your own personal cardiac expert on site, for example, but when you need one, you want the best cardiac expert ever. And that's what cloud services providers like AWS do. They're the best specialists you could ask for, but if you only borrow them when you need them, it's much less expensive. And if there was ever anything to delegate to experts who do nothing but that, whose livelihoods depend on being really good at it – it would be cyber security."

2. **Utility barriers to cloud migration are as much psychological as they are technical.** While some of the utility professionals we spoke with cited technical obstacles slowing their migration to the cloud, other industry experts suggested that the biggest barriers are, in fact, psychological.

   > George Hawkins of Moonshot Missions echoed this idea when he spoke about his tenure as CEO and General Manager of DC Water, noting that "I may know that cloud services providers like AWS are really good at this, but I don't know who they are, I've never met the people that are keeping us safe, and that can be unnerving compared to keeping everything in the server room upstairs that I can actually visit."

   Several industry professionals also suggested that utility staff may have a false sense of security when it comes to their current on-premises networks and practices, particularly when it comes to air gapping. The IT and cyber security experts that we spoke with agreed that it is critical that utilities segregate their business systems (e.g., billing, asset management) and control systems (e.g., SCADA, telemetry) as

much as possible, but also emphasized that it is impossible to be truly air gapped in our increasingly connected, digital world.

> As Rick Gruenhagen of Innovyze put it, “there are a lot of misconceptions about the security of air gapped networks – as soon as someone plugs in their iPhone to charge, you’re not air-gapped anymore.”

Finally, industry experts pointed out that many of us already rely on the security of cloud-based systems far more than we often realize in our day-to-day lives, including for mission-critical applications and sensitive personal data.

> According to Nick Nedostup, Chief Information Security Officer at Xylem: “Some organizations may be reluctant to move to the cloud without realizing they are already there. Take email systems, for example. A functioning and reliable email system is critical to business success, which is why so many organizations have moved email to the cloud already.”

3. **Manage your cyber assets like you manage your water assets.** While both utility professionals and other industry experts pointed to utilities’ lack of familiarity with cyber security principles and best practices as a major challenge in the industry, several stakeholders suggested that cyber security may not be as alien of a concept as it appears to be. In fact, they highlighted important parallels between how utility leaders manage their water, wastewater, and stormwater systems, and how they can or should manage their IT and OT systems.

   > For example, one of the most basic steps that any utility can take to improve their cyber security posture is to maintain an up-to-date inventory of their digital assets and devices, just as they do for their pipes, pumps, and plants. As Kevin Morley, Federal Relations Manager at the American Water Works Association (AWWA), put it, “you need to know the architecture of your cyber assets just like you need to know the architecture of your distribution or collection system – if you don’t have that, you’re shooting in the dark.” Meanwhile, George Hawkins at Moonshot Missions suggested that utility directors should approach cyber security risk in the same way that they address risk in their sewer networks or biological treatment systems, noting that “risk management is a language and perspective that utilities are very familiar with.”
   >
   > Similarly, industry experts stressed that utilities should engage with the broader community – utility peers, technology partners, expert consultancies, and industry associations – for managing cyber security, just as they do for managing leaks, water quality, and sewer overflows, among other things. As Nick Nedostup at Xylem suggested, “if you’re not already collaborating with or speaking to your

peers on cybersecurity, I encourage you to get involved in those conversations and discussions. When it comes to security, there are professionals to guide you – you're not alone, whatever it is that you're facing."

In particular, trusted industry partners will have an important role to play as the market evolves in helping utility staff identify technologies that meet certain cyber security requirements or standards, as well as to help them navigate and negotiate contracts and service-level agreements with their technology providers. Third-party purchasing and technology standards are common in other corners of the industry – e.g., NSF certifications and AWWA standards for pipes, valves, filtration media, etc. – but there are relatively few widely accepted or agreed-upon certification schemes for cyber security in the water sector. According to Andrew Ohrt, Resilience Practice Area Lead at West Yost Associates, "what would be really helpful is for industry organizations to advocate within the cyber security realm on behalf of their utility constituents to establish standards for contracting with cloud service providers – so that if an industry organization says that certain security provisions should be in a contract in order for a utility to sign it, utilities and vendors will both know that at a minimum, those provisions have to be in there."

But despite these parallels between the strategies and best practices required for managing water and cyber networks, industry experts emphasized that there are also crucial differences. Like the utility professionals we spoke with, other industry stakeholders noted that cyber security requires a shift in mindset and culture that extends across the entire organization, with utility staff taking on new roles and responsibilities in addition to their core duties as operators and stewards of water, wastewater, and stormwater infrastructure.

Andrew Ohrt at West Yost Associates, said it best: "Utility operators need to have a change in mindset. We often ask utilities if they consider themselves defenders of their infrastructure. They don't yet, but they need to in a world that is as networked as the world we live in now."

AWS cyber security resources for water utilities

Many of the cyber security concerns and topics discussed by utilities and industry leaders can be addressed using industry developed guidance and tools to support the understanding and implementation of cyber security controls for utilities of all sizes. The US EPA, CISA, National Institute of Standards and Technology (NIST) and trade organizations like the American Water Works Association (AWWA) offer resources that

align with the NIST Cyber Security Framework (NIST CSF). Specifically, the AWWA offers the Water Sector Cybersecurity Getting Started Guide to support small and rural utilities in improving their cybersecurity practices, in addition to tools and resources for larger utilities.

The NIST CSF applies to on-premises and cloud solutions. It offers a key set of standards, methodologies, procedures, and processes designed to align policy, business, and technology solutions to cyber risks, and with Section 2013 of America's Water Infrastructure Act of 2018 (AWIA). Section 2013 requires community (drinking) water systems serving more than 3,300 people to develop or update risk assessments and emergency response plans (ERPs).

There are six foundational cyber security controls in the AWWA Water Sector Cybersecurity Risk Management Guidance for Small Systems that can help utilities implement and mature their cyber security on-premises and when using cloud products and services, including:

1. **Cyber Security training and awareness** for employees, contractors, and third-parties that includes general security awareness and job-specific incident response training to educate staff to be aware of the indications of a potential cyber-attack, who to report to, and what immediate actions to take.
2. **Establish an asset inventory** to establish a baseline for network performance that could indicate a cyberattack, and support vulnerability management activities.
3. **Maintain data security compliance** as required by applicable laws and regulations and implement a privacy policy and cyber breach notification policy.
4. **Protect systems from unauthorized access or use** to prevent misuse of utility data and systems.
5. **Provide physical security** to limit the potential for unauthorized access and damage from such hazards as natural hazards, structure fires, and electrical outages.
6. **Secure network design** using best practices including logical separation and defense-in-depth to help mitigate the potential for an attack and the consequences of an attack.

An additional security consideration for water utilities is mechanisms for vetting the security of their supply chain. Utilities can approach supply chain risk management in multiple ways: reviewing and accepting security & compliance certifications such as FedRAMP, SOC 1, 2 and 3, ISO 27000 series, and/or others; issuing supply chain

security questionnaires to vendors; or using third-party security assessment tools such as the AWS Foundational Technical Review for cloud-based solutions.

Foundational cloud security for the water sector

With many water utilities investing in cloud applications for wastewater treatment services, mobile workforce management, asset edge analytics, customer service, and regulatory compliance, cloud security is imperative. Many utilities may not realize that the same core cyber security principles that apply to their on-premises systems also apply to cloud environments. In many scenarios, cloud technology offers more security features and controls than those applied in on-premises environments.

Many water and wastewater utilities have already implemented a cyber security program within their organization based on the NIST CSF or a framework that promotes the same concepts and best practices such as ISO/IEC 27103:2018. The NIST Cyber Security Framework (CSF) is supported by governments and industries worldwide as a recommended baseline for use by organizations, regardless of its sector or size. It is built on five (5) core functions: Identify, Protect, Detect, Respond and Recover.

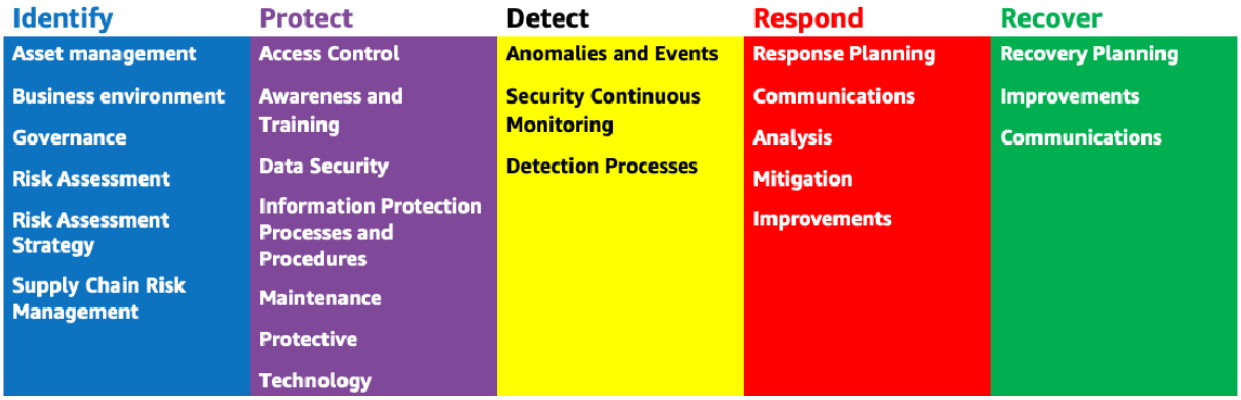

Figure 2 - NIST CSF Core Functions

The CSF offers a simple-yet-effective construct consisting of three elements – Core, Tiers, and Profiles. The Core represents a set of cyber security practices, outcomes, and technical, operational, and managerial security controls (referred to as Informative References) that support the five risk management functions – Identify, Protect, Detect, Respond, and Recover. The Tiers characterize an organization's aptitude and maturity for managing the CSF functions and controls, and the Profiles are intended to convey the organization's "as is" and "to be" cyber security postures. Together, these three elements enable organizations to prioritize and address cyber security risks consistent with their business and mission needs.

NIST CSF and AWS Best Practices

Amazon Web Services (AWS) understands the reliability objectives and security needs of water and wastewater utilities and works with them to meet their requirements at every stage of their cloud adoption journey. AWS delivers a scalable cloud computing environment designed for high availability and dependability, providing the tools that enable you to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of customer systems and data is of the utmost importance to AWS, as is maintaining customer trust and confidence.

The NIST Cyber security Framework (CSF) Aligning to the NIST CSF in the AWS Cloud whitepaper is a resource available to organizations of all sizes and industries wanting to understand how AWS cloud offerings align to the NIST CSF, and the role of third-party validations confirming AWS services' alignment with the NIST CSF risk management practices. Water utilities can use the whitepaper to evaluate enterprise-wide security posture and maturity, evaluate current and proposed products and services to help meet security objectives aligned to CSF categories and subcategories, and/or structure or restructure their security teams, processes, and training.

For utilities early in their cloud adoption journey, AWS also provides other best practice resources for customers adopting cloud technology including AWS Cloud Adoption Framework (AWS CAF), and the AWS Well-Architected Framework. These resources provide complementary tools to support organizations building or maturing their cyber security risk management programs, processes and practices using AWS. The NIST CSF whitepaper can be used in parallel with either of these best practice guides, serving as the foundation for your security program with the CAF or Well-Architected Framework as an overlay for operationalizing the CSF security outcomes when using cloud technology.

AWS Shared Responsibility Model

In a typical on-premises security model, customers are responsible for the end-to-end security in their data centers. AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and you are responsible for securing workloads you deploy in AWS (Figure 1). As an AWS customer you inherit the best practices of AWS policies, architecture, and operational processes built to satisfy the requirements of our most security-sensitive customers.

The utility assumes responsibility and management of the guest operating system (including updates and security patches) and other associated application software, as

well as the configuration of the AWS provided security group firewall. As shown in the chart below, this differentiation of responsibility is commonly referred to as security “of” the cloud versus security “in” the cloud.

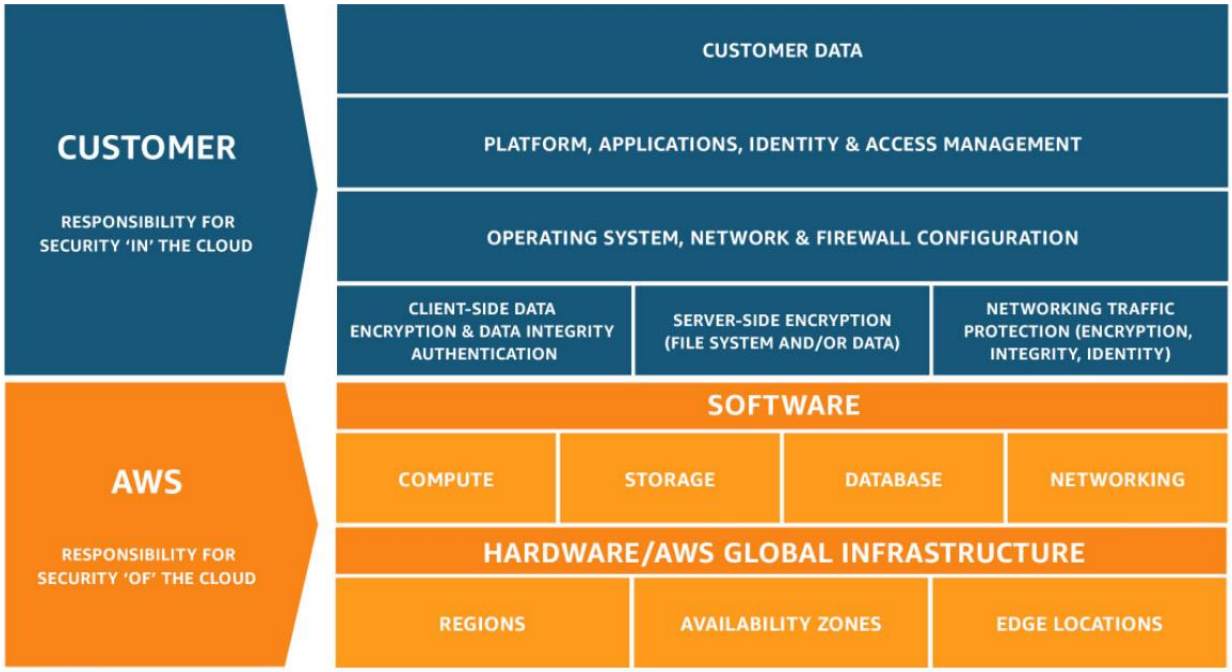

Figure 3 - AWS Shared Responsibility Model

Utilities purchasing solutions from AWS Partners should consider how the Shared Responsibility Model changes based on their specific use case, as the Partner may be responsible for security in the cloud controls. Understanding shared responsibility is fundamental to understanding the security and compliance of the cloud solution(s) deployed.

Shared Security Assurance

The principles of shared responsibility also extend to security assurance including who is responsible for achieving and maintaining accreditations and certifications. Figure 4 below illustrates that AWS, Vendors (including AWS Partners) and Customers have responsibility for obtaining and maintaining certifications. Utilities should be aware of these responsibilities when engaging with vendors and partners to purchase solutions.

Figure 4 - Shared Security Assurance

AWS Security Resources and Training

Cloud technology adoption may seem overwhelming to start, but AWS and its partners provide customers with guidance and expertise through online tools, resources, support, and professional services. Some examples are listed below, but the list is not exhaustive.

AWS Partner Network offers hundreds of industry-leading products that are equivalent, identical to, or integrated with existing controls in your on-premises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments, as well as hundreds of certified AWS Consulting Partners worldwide to help with your security and compliance needs.

AWS Professional Services houses a Security, Risk and Compliance specialty practice to help you develop confidence and technical capability when migrating your most sensitive workloads to the AWS Cloud. AWS Professional Services helps customers develop security policies and practices based on well-proven designs, and helps ensure that customers' security design meets internal and external compliance requirements.

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it simple to find, test, buy, and deploy software that runs on AWS. AWS Marketplace Security products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments.

AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. The AWS Well-Architected Framework includes a security pillar that focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events. Customers can use the AWS Well-Architected Tool from the AWS Management Console or engage the services of one of the APN partners to assist them.

AWS Well-Architected Tool helps you review the state of your workloads and compares them to the latest AWS architectural best practices. This free tool is available in the AWS Management Console, and after answering a set of questions regarding operational excellence, security, reliability, performance efficiency, and cost optimization, the AWS Well-Architected Tool then provides a plan on how to architect your cloud environment using established best practices.

AWS Reference Architecture examples and diagrams including **Smart Metering for Water Utilities**. The AWS Architecture Center provides reference architecture diagrams, vetted architecture solutions, Well-Architected best practices, patterns, icons, and more. This expert guidance is contributed by cloud architecture experts from AWS, including AWS Solutions Architects, Professional Services Consultants, and Partners.

Conclusion

As U.S. water utilities continue to adopt cloud technology to unlock historically siloed data, reduce total cost of ownership for IT operations, and improve the efficiency of their operations, they need to understand and implement cyber security controls that meaningfully reduce cyber risk. Through collaboration with AWS and AWS Partners, water utilities can standardize their security controls in alignment with industry frameworks and best practices.

Contributors

Contributors to this document include:

Eric Bindler is Senior Research Director for Bluefield Research, overseeing Bluefield's Digital Water and Municipal Water research services. His areas of expertise include digital water technology, company strategy, water finance and investment, and water and climate policy. He is also an active contributor to the Smart Water Networks Forum (SWAN), and was recently selected for a three-year term on the SWAN Council. Eric's in-depth analysis is often cited in the press, and he is a frequent panelist at global industry and corporate events. Eric holds a MA in Global Development Policy from Boston University.

Patrick Keaney is the worldwide head of business development for AWS Water, focused on bringing cloud technologies and services to the water market. Prior to joining AWS Patrick spent more than two decades as a global executive with Arcadis, a global engineering firm focused on water and environmental sustainability and resilience. His focus at AWS is to align internal AWS and partner teams to help solve critical water issues such as aging infrastructure, non-revenue water, and the public's understanding of the value of water. Patrick is working to deliver solutions such as predictive equipment condition assessments (Monitron), digital twins, and other AIML tools to water utility customers.

Kristine Martz is a member of the AWS security assurance team working as an energy and utilities sector industry specialist. She is a 10-year veteran of the energy and utility industry. Kristine helps utility customers adopt cloud solutions for regulated workloads in a secure and compliant way.

Further reading

For additional information, refer to:

- AWS Architecture Center

- AWS Glossary of Terms
- AWS Well Architected Framework Security Pillar
- AWS Security Best Practices
- AWS Foundational Security Best Practice Controls
- Power & Utility Path to Production Information Guide
- Executive's Guide to AWS Cloud Security
- Executive's Guide to AWS Security Control Domains
- AWS Shared Responsibility Model
- Best Practices for Security, Identity & Compliance

Document revisions

Date	Description
March 27, 2023	First publication