



Navigating NERC CIP compliance in the cloud

How new standards
are shaping energy
in 2024 and beyond

Contents

Page 3	Accelerating innovation and ensuring compliance for power and utilities leaders >
Page 5	Meeting change with transformation >
Page 6	Extracting value from data in the cloud >
Page 7	The imperative to innovate >
Page 8	Overclassification leads to opportunity cost >
Page 11	The evolution of NERC CIP compliance and the cloud >
Page 14	What NERC CIP changes mean for you >
Page 17	Managing a compliant transition >
Page 19	Shaping the future of NERC CIP standards >
Page 21	Powering a sustainable future together >
Page 25	Meet the authors >



Accelerating innovation and ensuring compliance for power and utilities leaders

It is no small feat to balance the relentless need for innovation with stringent compliance demands. Leaders are continuously navigating the complexities of integrating new technologies while adhering to regulatory frameworks like the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards.

The January 2024 updates to NERC CIP created even more opportunities for the power sector to use cloud technology, allowing storage of medium- and high-impact Bulk Cyber System Information (BCSI) in the cloud as long as certain requirements are met. Understanding the nuances of these changes is crucial for driving operational excellence and achieving sustainability goals.



A strategic compass for energy leaders poised to share the future of the industry.

In the following pages, we will:

- Demystify the intricacies of innovating in a compliance-driven landscape with [NERC CIP](#)
- Cover the January 1, 2024, changes to the NERC CIP Reliability Standards and how they could affect your organization
- Offer insights for effective integration of cloud solutions into your operations
- Discuss the future of NERC CIP Reliability Standards and how you can get involved

Whether you're at the beginning of your cloud adoption journey or looking to optimize your existing infrastructure to save costs and unlock innovation, this guide can help you chart a course through the dynamic landscape of digital transformation, facilitating security and compliance and aligning with industry-leading best practices.

A photograph of two utility workers, a woman and a man, wearing white hard hats and high-visibility yellow safety vests over plaid shirts. They are standing outdoors on a construction or industrial site, looking at a tablet held by the man. The background is a blurred landscape with hills.

Meeting change with transformation

Power and utilities companies are at the forefront of a transformative journey to connect renewables, grids, and people. The key to driving innovation and sustainability can be found in the data that already flows through your organization. With the advent of cloud platforms and AI, unlocking your data's insights isn't just a possibility—it's an imminent reality.

Cloud platforms like Microsoft Azure play a vital role in achieving your enterprise's potential. Digitization is paving the way for enhanced energy management, smart grid outcomes, improved customer engagement, and propelling the industry toward a net zero future. At the same time, the shift to data driven operations gives the industry the power to reimagine the way it operates, so together we can drive greater efficiency and fortify resilience in the face of diverse challenges.



Extracting value from data in the cloud

Integrating renewables

Seamless integration and management of renewable energy sources within the power grid.

Grid modernization

Operating an intelligent and secure grid, processing real-time grid conditions, and analytics with predictive monitoring capabilities.

Enhancing customer experience

Better decisions driven by deeper insights into customer behaviors and preferences.

Operational innovation

Predictive maintenance and scalable support that reduces downtime and creates efficiencies.

Security and compliance

Improved threat detection and security in compliance with NERC CIP.

IoT and edge computing

Real-time monitoring and control that improves resilience and unlocks distributed grid potential.



The imperative to innovate

Several shifts are converging to make this a dynamic moment in the power sector. The transition to clean energy is driving innovation in nearly every part of the business. Security threats are taking on new shapes and increasing in frequency. Digital transformation is modernizing infrastructure, introducing a new set of challenges. Concurrently, regulations continue to evolve in response to these industry changes, making compliance increasingly complex.

And yet, one imperative remains unchanged: providing accessible, uninterrupted, and secure power to customers across North America. The Bulk Electric System (BES) forms the backbone of our power supply, and its significance cannot be overstated. Disruptions or failures within the BES could have far-reaching impacts, affecting vast geographical areas and millions of lives.

The CIP requirements established by NERC aim to prevent potential disruptions by creating a secure and resilient BES. From the protection of electronic security perimeters to the management of system security, these standards ensure the reliable operation of North America's electricity grid. Compliance is more than meeting requirements; it demonstrates a commitment to safeguarding our modern way of life amid this era of change.

For NERC entities, moving forward with digital transformation while meeting CIP requirements presents as many opportunities as it does challenges.



Overclassification leads to opportunity cost

Although regulations are still catching up to technology, power and utilities companies can already unlock more value from the cloud by optimizing data classification.

Modern utilities generate and manage vast amounts of data, from consumer usage patterns to grid operation metrics to asset performance data. How NERC CIP classifications are applied to that data can influence where it's stored and how it's treated. Differentiating between BES Cyber System (BCS), BES Cyber System Information (BCSI), and non-BCS/BCSI isn't just about meeting NERC CIP requirements. It's also about prioritizing security measures and resources. Understanding what falls outside these categories allows utilities to adopt a more flexible approach, optimizing resources without compromising security.

When organizations overclassify datasets that do not fall within NERC's definition of BCSI, it can also cause unnecessary costs and lost value. When organizations erroneously classify data as BCSI, it triggers the need for expensive and stringent access controls, along

with documentation for audits, and can pose challenges when moving to cloud environments. Although the tendency to overclassify often stems from a well-intentioned desire to exercise caution and ensure compliance, it introduces complexities that may outweigh the intended benefits. Instead, power and utilities companies can optimize the efficiency and cost-effectiveness of their data management.

By taking a more accurate approach to classification, organizations can ensure that data is quickly accessible, analyzed, and acted upon, effectively streamlining operations while remaining compliant. Creating clear classification criteria, deploying tools that automate and validate data categorization processes, and training personnel in data management best practices can help strengthen overall compliance.



The task of correctly categorizing systems and data isn't a one-time exercise. In an ever-evolving technological landscape, organizations need comprehensive asset inventories, detailing each component's function, data flow, and interdependencies. Periodic drills, workshops, and assessments can also help reinforce your teams' knowledge over time. Third-party audits focused on classification can give companies the benefit of external perspectives. And as guidelines change, it's essential to make sure that these protocols are updated in tandem and socialized within the organization.

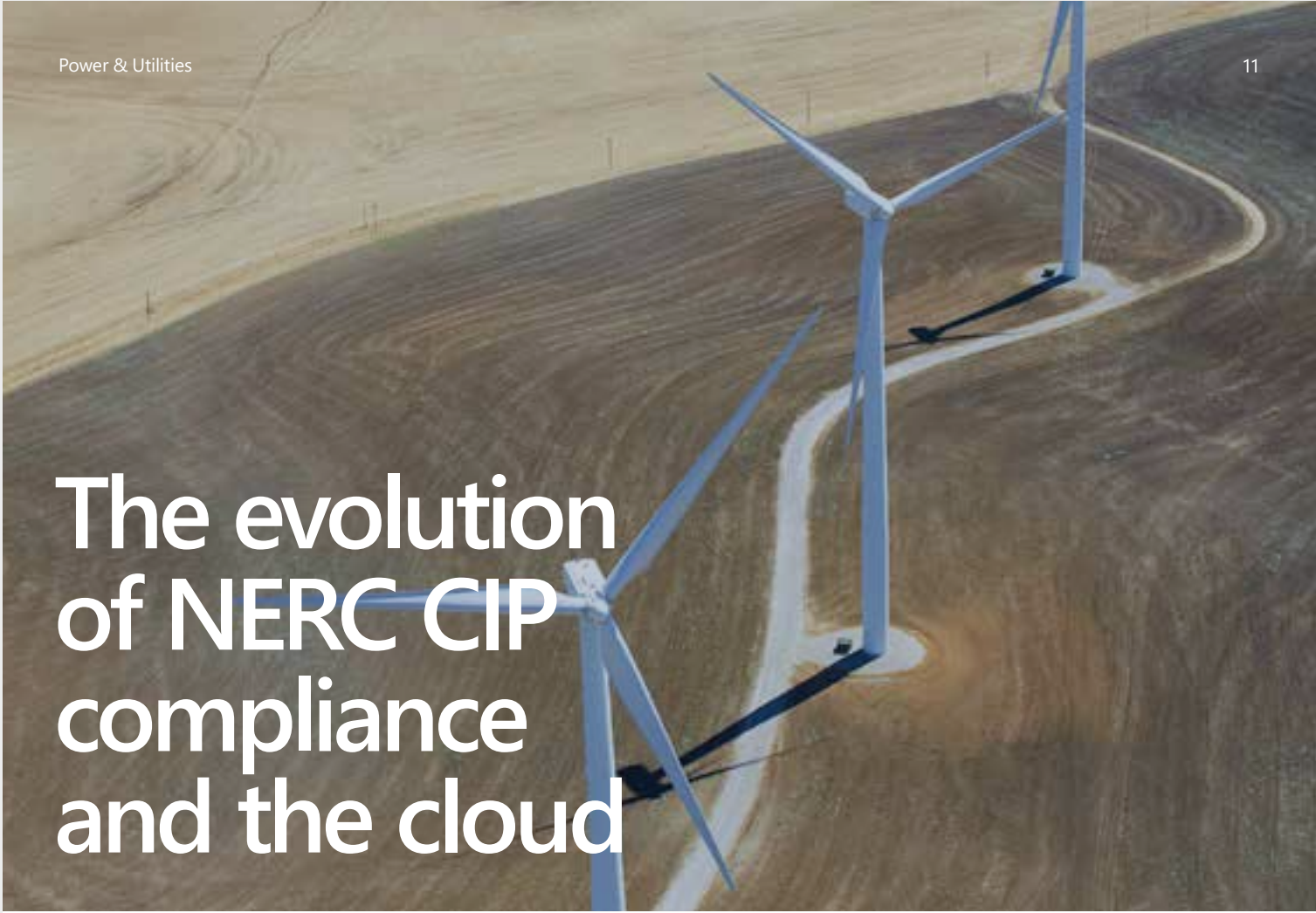
In practice, the effects of overclassification are evident in several scenarios within the power and utility sector. For instance, consider the treatment of distribution-related datasets, such as metering data or low-voltage asset information. While these types of data



often fall outside the scope of NERC CIP requirements, some utilities, erring on the side of caution or adopting a broad-brush approach to classification, categorize them as BCS. This conservative stance, while well intentioned, inadvertently restricts these datasets from leveraging cloud environments. In the cloud, they could benefit from enhanced processing power, sophisticated analytics, and more robust computational capabilities. By remaining on-premises due to overclassification, these valuable datasets are not utilized to their full potential, hindering opportunities for innovation and efficiency.

Another example can be seen in how high-voltage transformer data within a 230-kV substation is handled. Although the transformer itself, as a part of the BES, is subject to stringent protection requirements, the detailed operating characteristics, such as temperature, oil viscosity levels, and humidity, do not inherently require the same level of classification. If these operational parameters are overclassified, the utility misses out on the chance to use cloud-based solutions for predictive and preventative maintenance. By correctly categorizing this data, utilities can take full advantage of cloud capabilities to enhance asset management, reduce downtime, and optimize maintenance schedules.

These examples underscore the importance of nuanced and accurate data classification. It's not just about staying compliant; it's also about making informed decisions on data management that unlock the cloud's full suite of benefits. Accurate classification enables utilities to ensure compliance while being able to leverage the agility and innovation offered by cloud technologies, ensuring they are not just secure, but also strategically positioned for future advancements.

An aerial photograph of a wind farm. Two large, white, three-bladed wind turbines are visible, standing in a field of brown, tilled soil. A dirt road or path winds through the field, passing between the turbines. The background shows more of the field and some distant structures.

The evolution of NERC CIP compliance and the cloud

How power and utilities organizations classify their data has become increasingly important in light of two revised NERC CIP standards that went into effect on January 1, 2024. The updated guidelines allow storage of medium- and high-impact BCSI in the cloud if certain requirements are met. This milestone reflects a growing recognition of the advanced security and capabilities offered by cloud platforms like Azure. The changes align with the industry's need for greater flexibility, cyberresilience, and efficiency in managing critical infrastructure.

Although these revised standards empower companies to expand their use of cloud technologies, managing change can be intimidating. To help, cyberrisk management consultant Tom Alrich gives an at-a-glance view of what's changing.

Workloads that can be deployed in the cloud while maintaining CIP compliance

**Prior to
January 1, 2024**



Distribution systems and information about those systems

Any system that controls or monitors assets (for example, generating plants or substations) that are not classified as part of the BES is considered a distribution system. These systems, along with information about them, are not subject to NERC CIP standards, except for certain systems owned by distribution providers and listed in Section 4.1.2 of CIP-002-5.1a.

Low-impact BES Cyber Systems and information about those systems

In essence, these are systems that control and monitor the operation of BES assets (primarily control centers, transmission substations, and generating stations, including renewables installations) that are not classified as high-impact in Section 1 or medium-impact in Section 2.

**As of
January 1, 2024**

Distribution systems and information about those systems

Low-impact BES Cyber Systems and information about those systems

Medium- and high-impact BCSI

Workloads that cannot yet be in the cloud while maintaining CIP compliance

**Prior to
January 1, 2024**



Medium- and high-impact BCSI

Since NERC CIP Version 5 introduced the concept of BCSI in 2017, it has been effectively impossible for NERC entities to store BCSI for medium- or high-impact BES Cyber Systems in any cloud environment while remaining CIP compliant. The primary reason for this was that CIP-004 called for BCSI “storage locations” (that is, the physical devices on which BCSI was stored) to receive documented protections that no cloud service provider could ever document.

Medium- and high-impact Electronic Access Control or Monitoring Systems (EACMS)

Medium- and high-impact BES Cyber Systems (BCS)

Medium- and high-impact physical access control systems (PACS)

Deploying any of the four workload types listed above in the cloud would have made cloud service providers (CSPs) responsible for providing a huge amount of documentation—many millions of pages—that no CSP could have ever provided. Yet not providing it would have placed the NERC entity in violation of most of the NERC CIP requirements during the entire audit period.

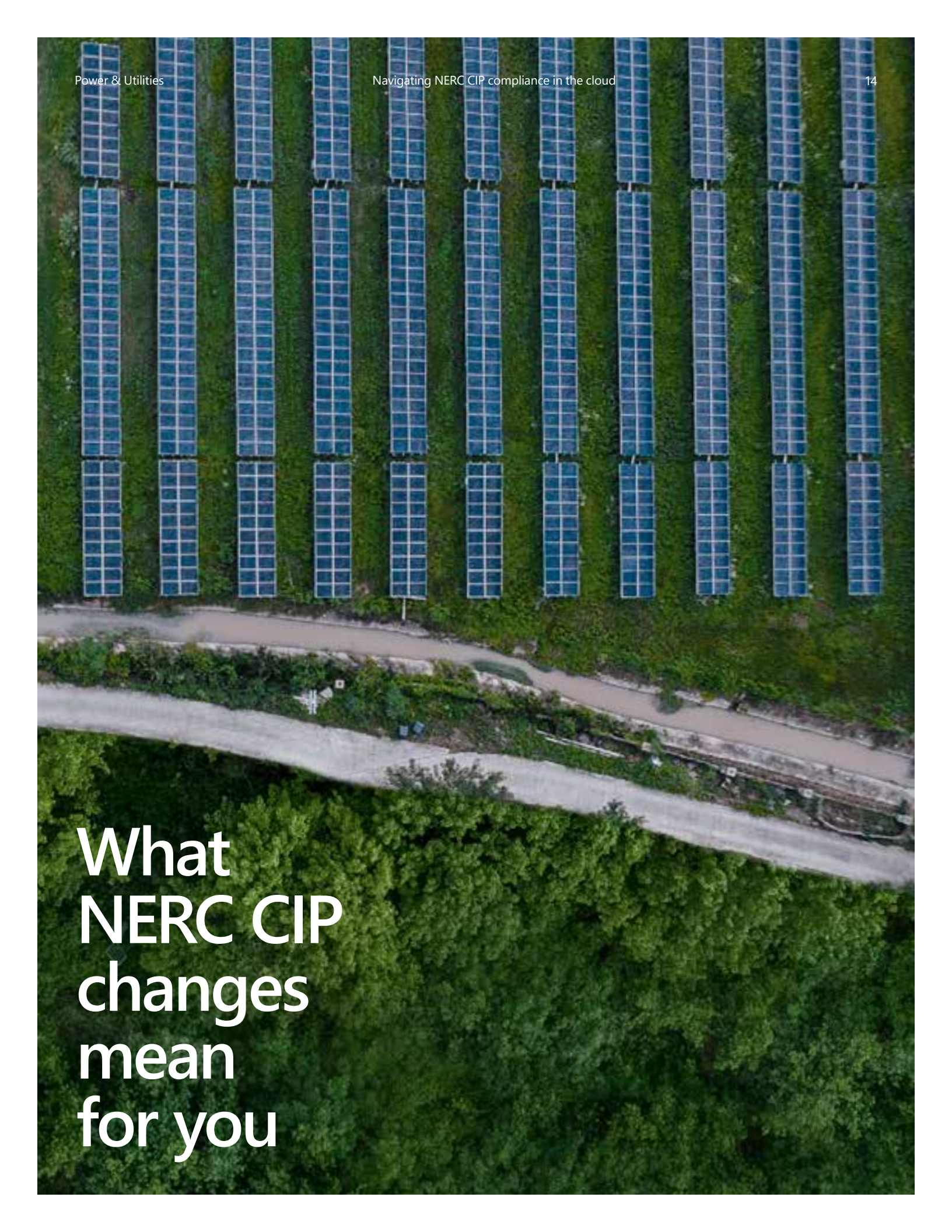
**As of
January 1, 2024**

Medium- and high-impact BES Cyber Systems (BCS)

Medium- and high-impact EACMS

Medium- and high-impact physical access control systems (PACS)

While the revisions to NERC CIP standards, effective January 1, 2024, facilitate greater flexibility for BCSI, these other workloads continue to be virtually impossible to deploy in the cloud while maintaining NERC CIP compliance.



What
NERC CIP
changes
mean
for you

The January 1, 2024, changes to NERC CIP give power and utilities companies the flexibility to further expand their use of cloud services, but there are risks in addition to rewards.

NERC-regulated entities will be able to store BCSI in Azure and other cloud platforms, fostering innovation and unlocking new operational capabilities. By transitioning data to the cloud, businesses can unleash optimized asset management, advanced load forecasting, and smoother integration of renewable energy sources, ultimately leading to better decision making and resilience.

Microsoft offers a [leading cloud for security](#) across information technology (IT) and operational technology (OT), with security resources, [tools](#), and best practices to support power and utilities companies. In an era increasingly shaped by AI, our investment in [cybersecurity innovation](#) is stronger than ever.

"As we enter the age of AI, it has never been more important for us to innovate, not only with respect to today's cyberthreats but also in anticipation of those to come."

Charlie Bell

Executive Vice President, Microsoft Security

Learn how [Microsoft's Secure Future Initiative](#) is building more secure foundations for the AI era and beyond.



However, cloud migration can pose challenges when not navigated with care. Inadequate planning and execution can lead to regulatory compliance issues, operational disruptions, and heightened cybersecurity vulnerabilities. A robust risk management strategy requires a holistic and proactive plan.

Start by engaging an experienced, trusted technology partner to explore the best configuration for your needs. It may be a good idea to shift investments into technology that supports encryption, secure access to BCSi in the cloud, and tools for monitoring and managing those environments. It will also be essential to bring your teams along with you. Update internal policies, access rights, training, and procedures to align with the new NERC CIP standards. Taking these steps can help ensure that you avoid unnecessary costs or interruptions.

“Let’s bring the best minds together to start approaching these problems differently, to focus on scale and repeatability and how we’re delivering these essential systems faster.”

Hanna Grene

Global Operations and Go-to-Market Leader,
Worldwide Energy and Resources Industry, Microsoft

See how [Schneider Electric and PG&E collaborated with Microsoft](#) to build a DERMS system fully built and deployed in the cloud.





Managing a compliant transition

The new CIP-004-7 and CIP-011-3 standards went into effect on January 1, 2024. Now NERC entities that own high- and/or medium-impact BCS will be able to store BCSI pertaining to those systems in Azure and other cloud environments as long as they take the required precautions. NERC CIP consultant Tom Alrich outlines the essential steps that entities must take to stay compliant in the cloud.

Information Protection Program (IPP) per CIP-011-3 R1

CIP-011-3 R1 requires the NERC entity to implement an “information protection program” for BCSI that includes:

- R1.1: Method(s) to identify BCSI.
- R1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.

In complying with R1.2, the NERC entity needs to specify how it will protect BCSI that is stored in the cloud. By far the most widely used technology for this purpose will be encryption of the data, both during storage in the cloud and during transmission to and from the cloud.

Managing BCSI access per CIP-004-7 R6

CIP-004-7 R6 is a new requirement that prescribes three procedures that the NERC entity must have in place (and must have described in its Information Protection Program for CIP-011-3 R1) to manage “provisioned access” to BCSI, including both physical and electronic BCSI. For electronic BCSI, the individual with access must be able to “use” the BCSI, which means the person is able to view encrypted data in unencrypted form, perhaps because they have been provided with access to the encryption keys. If the individual can view the data in its encrypted form but cannot decrypt it, they are not considered to have provisioned access to the data.

To comply with CIP-004-7 R6 with respect to persons with unencrypted access to BCSI in the cloud, the NERC entity must document and implement programs to do the following:

- Provision access to unencrypted BCSI in the cloud based on need (R6.1)
- “Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI”
 - “Have an authorization record” (R6.2.1)
 - “Still need the provisioned access to perform their current work functions, as determined by the Responsible Entity” (R6.2.2)
- “For termination actions, remove the individual’s ability to use provisioned access to BCSI by the end of the next calendar day following the effective date of the termination action” (R6.3)



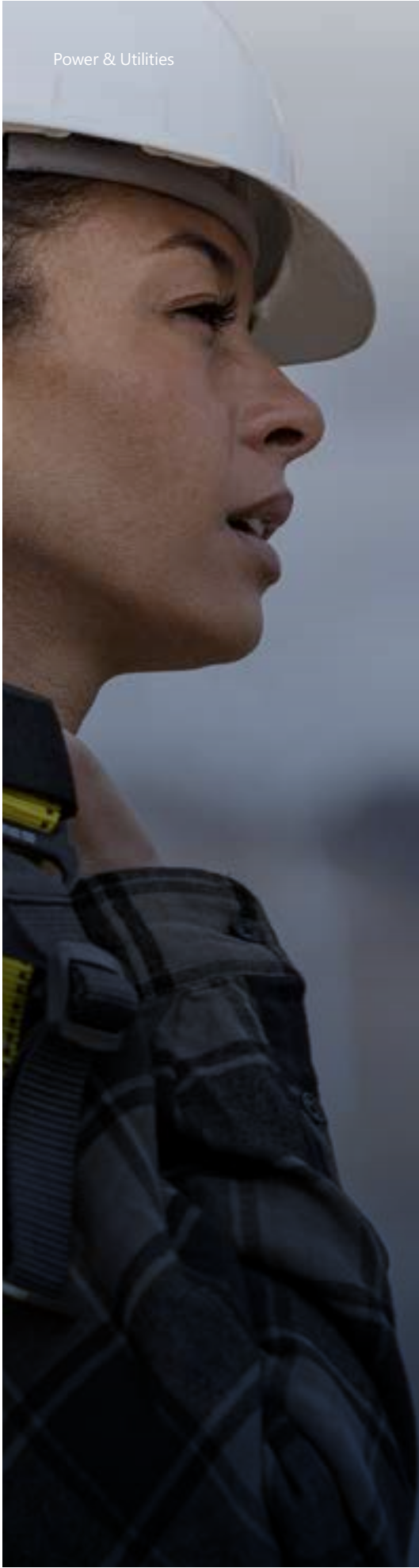
Shaping the future of NERC CIP standards

The latest revisions to the NERC CIP standards, while modest, mark an important step toward aligning regulations with modern technology.

When the NERC Standards Committee approved a Standards Authorization Request (SAR) in December 2023, it marked a cornerstone in the journey toward fully normalizing cloud use within the scope of NERC CIP standards. Over the next several years, the initiative is likely to bring about significant revisions to the CIP standards and possibly the NERC Rules of Procedure too. There is a wide consensus across the NERC community—including NERC entities, staff of the Electric Reliability Organization, and vendors serving the power industry—that this evolution is overdue and critical for the industry's progress.

The precise outcomes of this process will be shaped over time and with input from a broad spectrum of stakeholders. NERC entities are encouraged to actively participate in drafting teams, vote, and provide feedback on new drafts. This invitation is also extended to all stakeholders, including cloud service providers, other vendors, and indeed any electricity user in North America. Participation can take various forms—attending drafting team meetings (both in-person and virtual), joining mailing lists, or engaging in related discussions on platforms like LinkedIn and Energy Central. It's also worth noting that the NERC Standards Drafting Teams are composed entirely of volunteers from NERC entities. Although becoming a voting member demands a significant time investment, it often proves to be an immensely rewarding experience.

With everyone's support and input, all types of NERC systems, including medium- and high-impact BCS and EACMS, could be deployable in the cloud within three to four years.



Microsoft is at the forefront of this evolution, actively collaborating with energy sector and regulatory groups to help ensure a cloud-based future that's secure, compliant, sustainable, and resilient.

Through these collaborations, Microsoft is dedicated to guiding the power and utilities sector through this ever-evolving landscape, facilitating a seamless integration of advanced cloud and AI technologies into their regulatory and operational frameworks.

A young child with blonde pigtails is shown in profile, focused on working on a solar panel. The child is wearing a white sleeveless shirt. The background is a blurred view of a solar farm with rows of panels stretching into the distance under a clear sky.

Powering a sustainable future together

Taking the next step in your digital transformation journey can be daunting, but you don't have to do it alone. At Microsoft, we are committed to guiding you every step of the way. Move toward your organization's vision of the future with Microsoft's power and utilities team—leaders who have been in your shoes and understand your complex operational environment.

Strategic partnerships are the key to developing the right digital strategy across IT and OT. There isn't a one-size-fits-all solution for achieving a secure and interconnected future, especially for an industry as nuanced and critical as power and utilities. Our team can help define your organization's unique requirements and align them with the appropriate cloud offering. Options range from public clouds like Azure, known for vast scalability, to hybrid solutions such as Azure Arc, which balance on-premises infrastructure with the agility of cloud computing.

Innovate with confidence that our industry-leading solutions can help keep your data safe and compliant, as regulations continue to evolve. Navigating the industry's shifting landscape might seem daunting, but together we can harness your organization's potential for operational excellence and long-term growth.

Learn more about [powering an innovative future with Microsoft](#). >



“We couldn’t
survive without
the cloud.”

Sergiy Galagan

Chief Information Officer, NPC Ukrenergo

As Ukraine’s power plants became a primary target of political action, National Power Company Ukrenergo fought diligently to maintain the energy supply for Ukrainians. As 8,000 employees worked tirelessly to repair their generating facilities, they turned to Microsoft to support their critical infrastructure in the cloud.

Read more to learn [how Ukrenergo secured and reestablished the grid during the war in Ukraine.](#)



Leading security solutions for power and utilities companies

Microsoft is recognized as [best-in-class across the security suite](#). With more than 100 compliance offerings worldwide, our unparalleled investment in security is powering innovation in the energy industry and beyond.

Microsoft Defender for IoT

Get real-time asset discovery, vulnerability management, and cyberthreat protection for your Internet of Things (IoT) and infrastructure.

[Learn more >](#)

Microsoft Security Copilot

Improve security outcomes at machine speed and scale with AI-powered, natural language security analysis.

[Learn more >](#)

Microsoft Sentinel

Uncover sophisticated threats and respond decisively with an intelligent, comprehensive security information and event management (SIEM) solution.

[Learn more >](#)

Microsoft Azure

Maximize your existing assets while operating for the future with comprehensive and highly secure cloud platform.

[Learn more >](#)

Simplify the complex with analyst-recognized cybersecurity



[Zero Trust >](#)



[Identity and network access >](#)



[Information protection and governance >](#)



[Risk management >](#)



[Secure remote work >](#)



[Cyberthreat protection >](#)

Meet the authors



Bilal Khursheed

Worldwide Power and Utilities Leader,
Energy and Resources Industry, Microsoft

With nearly two decades at the forefront of the power and utilities industry, Bilal Khursheed partners closely with global power and utilities leaders, governments, policy makers, and OT solution providers to shape the future of the energy industry. His diverse leadership roles have spanned transmission and distribution, nuclear operations, and the pivotal realm of digital transformation. Renowned for merging innovation with tangible results, Bilal drives Microsoft's global power and utilities vision, championing sustainability and mentoring the next generation of industry leaders.



Tom Alrich

NERC CIP Compliance and Supply Chain
Security Consultant

Tom Alrich is a well-known consultant, [blogger](#), and author of the new book *An Introduction to SBOM and VEX*. Tom has been consulting on NERC CIP and supply chain cyber risk management since 2008, working previously for Honeywell and Deloitte.



©2024 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.