SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 1 | January 2026 - Peer Reviewed Journal

FROM COMPLIANCE TO CULTURE: ASSESSING ORGANIZATIONAL CYBERSECURITY READINESS IN PUBLIC VS. PRIVATE U.S. UTILITY COMPANIES

Benjamin Panful [a], Barnabas Apaflo [b], Nasiru Hutchful [c]
[a] *Lake Land College, USA*
[b] *Texas A&M University*
[c] *Department of Computer Science and Engineering, University of Mines and Technology, Ghana*

**Corresponding Author: Nasiru Hutchful*

Article DOI: https://doi.org/10.36713/epra25731
DOI No: 10.36713/epra25731

ABSTRACT

The United States (U.S.) utilities are increasingly being deployed in convergent information-technology and operational-technology settings putting vital energy and water systems at risk due to advanced cyber-attacks. Federal and state regulators have added to compliance mechanisms over the past decade, most notably the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards, Environmental Protection Agency (EPA) cybersecurity guidelines, and the Cross-Sector Performance Goals by the Cybersecurity and Infrastructure Security Agency (CISA). However, as cases of inadequate adherence continue to emerge, formal compliance cannot be a very reliable approach to creating resilient organizations. This policy-oriented literature review on the identification of the differences between public utilities and private utilities in terms of translating regulation compliance to a sustained culture of cyber readiness was integrative in nature. The study synthesizes the evidence on governance structures, workforce, and leaders' accountability in different sectors based on peer-reviewed and policy resources. The results suggest that on the one hand, the public utilities tend to focus on the required controls and reporting, whereas on the other hand, the private utilities tend to be more adaptive and risk-driven with the support of the learning cultures based on the leadership. One of the most important findings of the review is the cross-sector analysis between compliance maturity and cultural transformation providing practical advice to regulators and utility executives to achieve the balance between oversight and innovation. At the end of the paper, recommendations are provided on how to incorporate culture metrics in the national policy frameworks on cybersecurity in the utility sector.

KEYWORDS: *Cybersecurity readiness, Compliance and governance, Organizational culture, Critical infrastructure resilience, U.S. energy and water sectors.*

1. INTRODUCTION

The digitalization of U.S. utilities has increased both the performance and coverage of critical services and, at the same time, has increased vulnerability to cyber-physical threats. Smart-grid devices, interconnected control systems and water-treatment automation have provided them with complex attack surfaces, which require technical and organizational readiness. Empirical syntheses from the energy sector consistently show that employee awareness gaps, susceptibility to social engineering, and weak security culture remain persistent contributors to cybersecurity failures, even where formal controls are well established (Panful et al., 2025). Companies in the public sector that provide utilities like water and power functions under strict statutory requirements like the Environmental Protection Agency (EPA) Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems and Federal Energy Regulatory Commission Critical Infrastructure Protection (FERC CIP)-aligned orders where compliance verification and auditing are prioritized (EPA, 2024a; FERC, 2023b).

Whereas private utilities are also subject to much of the same reliability requirements, they are more likely to supplement regulation with voluntary frameworks such as National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0 and International Organization of Standardization/ International Electrotechnical Commission (ISO/IEC) 27001, employing internal governance to make cybersecurity consistent with business resilience.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 1 | January 2026 - Peer Reviewed Journal

Nevertheless, it is always found that research makes a clear distinction between compliance-based conformance and culture-based readiness. Compliance guarantees the least satisfaction in regulations, whereas culture motivates an unending learning process, staff empowerment, and sophisticated defensive processes (Folorunso et al 2024).

Research on organizational behavior in critical infrastructure has recorded that check-the-box compliance can meet legal requirements and leave some underlying socio-technical vulnerabilities unchecked. According to Lin and Saebaler (2019), the excessive exposure to compliance by utilities exists at the expense of risk-based decision-making, which would form an artificial dichotomy of compliance and resilience. Their observation highlights the need to change compliance as endpoint to culture as continuum.

This transition is becoming recognized by federal and state structures. The CISA Cybersecurity Performance Goals and its complementary document, Culture of Cyber Readiness help leaders to incorporate security awareness and responsibility at all organizational levels (CISA, 2023). Likewise, the Cybersecurity Considerations of Distributed Energy Resources of the Department of Energy (DOE) introduces the idea of security-by-design as a cultural requirement and not a compliance requirement (DOE, 2022). Nevertheless, according to the Government Accountability Office (GAO) report on the cybersecurity oversight of utilities, the public utilities do not possess the capacity to govern themselves to implement federal policies as a consistent organizational practice (GAO, 2024). This difference leads to questioning how compliance structures and cultural conditions contribute to cybersecurity readiness in both U.S. utility companies, private and public. Recent case-study evidence of SCADA and OT breaches in U.S. water utilities underscores how technical vulnerabilities—such as exposed HMIs, default credentials, and weak remote-access controls—persist despite formal compliance frameworks, highlighting the gap between regulatory adherence and operational resilience (Panful, Apaflo, & Hutchful, 2025).

The significance of this is a two-sided character of U.S. critical-infrastructure governance. Public utilities are subject to showing accountability to taxpayers and regulators whereas the response of the utility in the market and the shareholder is the main focus of the private utility. They therefore vary in their motivations, investment patterns, and involvement in the workforce (NARUC, 2019). Prescriptive controls are commonly applied by public utilities with constrained budgets and old systems, and a more adaptive risk-based controls are executed by the private, with less obligatory cultural evaluations (CRS, 2025). According to Folorunso et al. (2024), security compliance is essential in defining and improving the cybersecurity position of an organization and its effectiveness will depend on the level of integration into everyday practice.

The expanding body of literature builds upon this observation into new areas including the Internet of Things (IoT). Bonsu et al. (2025) show that compliance frameworks that are promoted by policy can enhance the lowest levels of protection, but they need to transform to become shared values that inform organizational behavior. Applied to utilities, the same reasoning can be observed. Regulatory mechanisms such as NERC CIP are necessary to offer much-needed structure, however, only coupled with cultural support such as leadership commitment, employee-competence, and interdepartmental coordination, can readiness be seen as profound. The World Economic Forum (WEF) also claims that the issue of cyber resilience in electricity ecosystems relies on the leadership accountability and collaborative culture (Martel et al., 2019).

This paper, therefore, aims to achieve two objectives. First, it incorporates scholarly and policy literature to contrast compliance-based and culture-based readiness in terms of their occurrence in both the public and the private utilities. Second, it suggests policy and managerial levers that could allow overcoming the compliance-to-culture gap. The paper utilizes integrative review approach, which involves the use of regulatory texts and the scholarly discussions of the frameworks of organizational culture and readiness. It compares evidence over the levels of governance, which enhances the knowledge of the way in which rule compliance develops into durable security culture in critical-infrastructure organizations.

2. COMPLIANCE-BASED READINESS IN PUBLIC AND PRIVATE UTILITIES

The tradition of regulations and audit-based accountability anchors cybersecurity preparedness in the U.S. utility sector. In the case of public utilities, especially in the energy and water industries, the compliance framework like the NERC CIP standards and the EPA cybersecurity standards can be used as the main tools in the governance of security operations. These frameworks provide a prescriptive foundation through which the management of access, response to incidents, and monitoring of systems is planned so that utilities can comply with enforceable minimum standards to secure critical assets (Moore, 2015; FERC, 2023b).

The nature of public utilities is highly regulated, and in such context, compliance with legal requirements can often be the determining factor regarding their cybersecurity stance. An example of such regulation is a directive by the EPA about water and wastewater systems that require thorough risk evaluation, entry and exit control, and contingency measures to meet the statutory requirements of the Safe

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 1 | January 2026 - Peer Reviewed Journal

Drinking Water Act (EPA, 2024a). However, studies show these utilities, especially small municipal systems, often do not have technical and financial means to sustain compliance without federal aid leading to the practice of the non-uniform implementation across jurisdictions (CRS, 2025).

Further evidence of the compliance-focused stance taken by the public utilities exists in other water-related evidence. The Water and Wastewater Systems project of the NIST National Cybersecurity Center of Excellence (NCCoE) reveals the unaddressed vulnerabilities of incomplete assets inventories, old-fashioned PLCs that cannot be updated, non-segmented network, and unrelated remote-access control, all factors that make compliance even more difficult and increase cyber vulnerability in resource-constrained public utilities. The report underscores the fact that a large portion of facilities rely on old network setups, manual configurations, and lack of network segmentation, all of which support a reactive and not an adaptive security posture (McCarthy et al., 2023).

Such compliance paradigm is also supported by government oversight. The U.S. Government Accountability Office found that there was disjointed coordination of federal agencies, which resulted in uncoordinated readiness to cybersecurity across sectors (GAO, 2024). The interactive guide of the National Association of Regulatory Utility Commissioners (NARUC) gives state regulators a set of assessment questions arranged in an ordered manner to determine whether the utilities adhere to governance, incident management, and risk-mitigation practices, which represents an institutional orientation towards checking compliance, rather than an ongoing improvement (NARUC, 2019). This compliance-oriented culture, which works well in standardizing baseline defense, can frequently create a level of procedural rigidity that constrained innovation and adaptive resilience.

On the contrary, private utilities are managed by hybrid governance frameworks that imply mandatory reliability regulations in addition to voluntary ones, including the NIST Cybersecurity Framework and the Secure Software Development Framework (SSDF). Such tools encourage the idea of risk-based governance and focus on flexibility, where organizations can align cybersecurity with the overall business objectives instead of regulatory minimums (NIST, 2024; Souppaya et al., 2022). This flexibility facilitates the incorporation of governance, technology, and workforce efforts in enterprise risk management. Policy reviews have underscored that these frameworks are frequently used by private utilities to integrate security controls across the modernization initiatives with the primary focus on secure-by-design and proactive minimization of risks as opposed to compliance documentation (DOE, 2022; NASEO, 2020).

Irrespective of such maturity, the public and the private utilities have limitations in operationalizing compliance into actual preparedness. The Cross-Sector Cybersecurity Performance Goals created by the Cybersecurity and Infrastructure Security Agency explain that compliance must merely be the minimum level of maturity and not the limit of performance (CISA, 2023). Recent research confirms that compliance is an essential yet incomplete part of security and to be cautious that organizations using it as a checklist practice overlook the larger human and cultural aspects required to be resilient (Folorunso et al 2024). This disjunction is also evident in the utility setting, where the controls are well documented, but the operational staff does not consistently engage in behaviors that can be seen to be cultural alongside the criticism that compliance without culture leads to nominal protection, as opposed to operational resilience (Lin and Saebeler, 2019).

The infusion of NERC CIP controls on electric utilities also indicates the complexity of operation in ensuring compliance. According to the SysAdmin, Audit, Network and Cybersecurity (SANS) overview, utilities have to balance the utilities between the business-level and operational needs and the agile compliance with the intricate CIP requirements, and such a misalignment may lead to fines or reliability issues. The document goes further to emphasize that the supply-chain requirements of the CIP-013 such as vendor-incident notification, remote-access revocation, and software-integrity verification adds more procedural burdens that reinforce the compliance-heavy stance of the sector (Conway et al., 2024).

In general, compliance-based readiness is adequate due to legal accountability and preliminary hygiene but is not as robust as they are needed in dynamic threat settings. Audit transparency is attained but there is usually lack of adaptive capacity in the public utility, and in the case with the private utility where compliance is embedded in the wider scope of governance that promotes innovation. The two sectors, however, need cultural mechanisms to perpetuate and internalize such technical and procedural standards.

3. CULTURAL READINESS INITIATIVES IN PUBLIC AND PRIVATE UTILITIES

Cultural readiness is the change in cybersecurity to be more of a value and not merely a routine requirement that may exist in governance and operations (Georgiadou et al., 2022). The situational awareness and preemptive defense behaviors within this paradigm are maintained by the employees, the leadership and the stakeholders who are in unity in complementing the formal controls. Scholars constantly note that compliance is supported by culture, otherwise, cybersecurity is not sustainable (Georgiadou et al., 2022).

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 1 | January 2026 - Peer Reviewed Journal

It has been proved with evidence that leadership commitment, employee empowerment, and training are key to the development and maintenance of such culture by several studies. Companies incorporating cybersecurity concepts into their daily operations, by educating, incorporating accountability schemes, and maintaining open communication gain a higher incident-response harmony and risk perception (Willie, 2023; Said et al., 2022). Similar association is found in the studies of cybersecurity capacity building, which emphasize that the apparent endorsement of top management serves as a final determinant of successful behavioral implementation (Uchendu et al., 2021).

The federal initiatives incorporate these cultural aspects to a greater extent in their directions. The Culture of Cyber Readiness program developed by CISA helps the organization to promote employee awareness, executive support, and leadership responsibility (CISA, 2023; CISA, 2021). On the same note, the Secure Your Business program offers practical cultural measures that small and medium-sized organizations can implement, and it advances to situations of public utility, which means that the implementation must be a continuous process and not a single workshop (CISA, 2025). The water-utility guidance and the NIST frameworks also consider the workforce competence as one of the most important determinants of resilience, with culture viewed as the source of bridging policy compliance and operational effectiveness (EPA, 2024a; NIST, 2024).

Cultural determinants of readiness include workforce competence, which is supported by water-sector cybersecurity maturity assessment evidence. According to a recent sector research, utilities that had a better level of protection are always characterized by organized employee training, rigorous access control rights and strict operational segregation of SCADA elements. The paper finds that the highest possible protection level is reached only when utilities apply other cybersecurity technologies besides all best practices, which emphasize that technology and culture should develop together in the case of resilience (Moraitis et al., 2023).

The private utilities are more inclined to promote cultural readiness by integrating their governance as well as initiatives by their leadership. According to the study conducted by the World Economic Forum on cyber resilience in the electricity ecosystem, executive ownership and cross-functional cooperation are the determinants of the culture integration in large energy firms (Martel et al., 2019). Cybersecurity awareness and certification programs tend to be part of the performance management of investor-owned utilities, and this practice is aligned with the cultural objectives and both shareholder and reputational-based incentives (NASEO, 2020).

This is extended by greater conceptual work across sectors. Research on policy-based security frameworks asserts that the protection of compliance frameworks can be assured in the long term only when institutionalized as values shared by the entire population, which supports the accountability and shared responsibility (Bonsu et al., 2025). This cultural connection is also evident in sustainability and smart-city studies, in which trust, transparency, and civic engagement come out as the foundations of digital-infrastructure resilience (Berlilana et al., 2021; Grigg, 2025). The use of complementary evidence by CISA implementation checklist and national-lab recovery guides, proves that regular exercises, training, and simulations strengthen the behavioral norms, and preparedness is solidified beyond compliance (EPA, 2024b; Whyatt et al., 2021).

All the literature reviewed describes culture as the crucial platform on which compliance grows into readiness. Whereas the public utilities depend largely on the federal programs and control to influence the cultural behavior, the private utilities are the ones to incorporate the same into the governance system and through the power of leadership. The difference highlights a systemic difference in incentive, i.e. public accountability versus competitive tenacity. Nonetheless, both industries move closer toward hybrid models which integrate both regulatory strictness and long-term cultural immersion. Utilities find themselves in a more adaptive cybersecurity stance with preparedness being not just concerning written processes but also regarding common skill and shared accountability.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 1 | January 2026 - Peer Reviewed Journal

4. CROSS-COMPARISON OF COMPLIANCE AND CULTURE-BASED READINESS MEASURE

Table 1: Measure compliance and cultural-based readiness between public and private utilities

Measure	Public Utilities	Private Utilities
Regulatory Environment	Run on compulsory prescriptive requirements including the NERC CIP rules and EPA cyber-guidelines. Compliance is audit-based, enforced externally, and demonstrably oriented towards conformance (Moore, 2015; FERC, 2023b; EPA, 2024a).	Under the same minimum reliability requirements but is not restricted by rigid, risk-based standards like NIST CSF 2.0 and SSDF 800-218. Governance is dedicated to proportionality and risk management according to the business (NIST, 2024; Souppaya et al., 2022).
Governance & Accountability	The process of governance is mostly compliance-based and externally controlled by federal or state authorities; the accountability is decentralized and dispersed among departments, and the success in the inspection is the main measurement of accountability (GAO, 2024; NARUC, 2019).	Cybersecurity is a component of governance that incorporates enterprise-risk management, accountability of the boards, and performance indicators associated with resilience performance (NASEO, 2020).
Leadership Engagement	Their involvement with the executive is usually reactive, where the executives respond to governmental deadlines, as opposed to cultural leadership (CRS, 2025).	Leadership is a strategic cybersecurity value; the senior management is the sponsor of continuous improvement and inter-functional cooperation (Martel et al., 2019).
Workforce Awareness & Training	Mandatory training programs under compliance frameworks but with inconsistent funding or updates, awareness maintained by toolkits at federal and external workshops (EPA, 2024b; CISA, 2021).	Training as a part of organizational development and performance evaluation. Regular training through simulations and certifications help to solidify the learning culture (Whyatt et al., 2021; Willie, 2023).
Incident Response & Operational Continuity	Protocols of response recorded to comply with audit reviews, the frequency of testing is restricted by the resources (CRS, 2025).	Enterprise resilience program Incident-response maturity. Through repeated exercises, learning and adaptive recovery become institutionalized (NASEO, 2020; Whyatt et al., 2021).
Technology Integration (Secure-by-Design)	Its implementation was usually postponed until required by the regulators, upgrades were limited by the old systems (EPA, 2024a).	Modernization and distributed-energy projects are defined by secure-by-design and align technical innovation with risk reduction (DOE, 2022; Souppaya et al., 2022).
Culture & Behavioral Readiness	Federal campaigns are externally instigators of cultural change. The use of checklists prohibits profound adoption of behavior (CISA, 2023; Folorunso et al 2024).	Culture that is internally developed based on leadership example, incentive, and collective responsibility. Cybersecurity is viewed as corporate identity (Georgiadou et al., 2022; Said et al., 2022).
Resource Capacity	Reliant on government funding cycles and federal aid. The funding limit continuous improvement (GAO, 2024; CRS, 2025).	Increased availability of personal investment and technical skills allows flexible adaptation and staff specialization (NASEO, 2020).
Incentive Structures	Out of regulatory compliance and the risk of sanctions, there is less financial incentive in surpassing the minimum standards (FERC, 2023b).	Under the leadership of performance measurements, reputation, and probable incentive-rate treatments of voluntary cybersecurity investments (FERC, 2023a).
Policy Evolution Trend	The shift to prescriptive to the hybrid models of readiness with a focus on culture and resilience (CRS, 2025; GAO, 2024).	Moving to combined governance that includes assurance of compliance with innovation and active prevention of threats (Bonsu et al., 2025; Grigg, 2025; Berlilana et al., 2021).

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 1 | January 2026 - Peer Reviewed Journal

A structural divergence can be identified in the comparison. Public utilities exhibit a high level of procedural adherence and open accountability, yet, they have no autonomy and resources to promote internal cultural change. Their maturity level of readiness reaches audit compliance, which is limited by the clunky systems and reliance on external control. Conversely, the private utilities convert regulatory expectations into strategic programs and impose cybersecurity on governance and workforce systems. They are more flexible, have higher investment capacity and leadership initiative which hastens the transformation between compliance and culture.

However, the two sectors have a common trend of moving towards converging hybrid readiness directions. The incorporation of culture measures in performance objectives as highlighted by federal policies and cross-sectoral models is a demonstration of how there is a transformational approach between reactive compliance and adaptive resilience. This change makes culture the maturity phase of operation whereby regulatory expectation and organizational behavior complement each other (Folorunso et al 2024; Georgiadou et al., 2022; CISA, 2023).

5. SYSTEMIC BARRIERS HINDERING THE CULTURE SHIFT

Although there are significant advances in regulations, compliance-based control has not yet changed to culture-based readiness throughout the utilities in the United States. Literature is dominated by three main barriers, such as structural fragmentation, resource disparity and behavioral inertia. Studies of cybersecurity audits further show that identifying control gaps and enforcing compliance does not necessarily translate into improved resilience unless behavioral accountability and leadership involvement are embedded in operations (Onyekwuluje et al., 2025).

Structural fragmentation is caused by duplication of mandate and irregular supervision. It is reported that utilities need to maneuver between conflicting requirements by FERC, EPA, DOE and CISA, which focus on various performance results. Such a patchwork of instructions makes it complex to implement and leads to the development of checkbox mentality in which utilities are concerned with audit pass rates rather than integrated resilience (GAO, 2024; CRS, 2025). This pattern aligns with broader energy-sector reviews indicating that socio-technical vulnerabilities frequently persist beneath formally compliant governance structures (Panful et al., 2025). This lack of a common framework of national oversight implies that cultural projects frequently become discretionary, as opposed to systemic priorities, especially to small or municipally owned entities.

This fragmentation is summed up by resource disparity. Public utilities often have limited budgets as well as outmoded infrastructure such that there is very little room to develop the workforce sustainably or modernize it. Federal tests observe that on the side of water and energy providers, there is a strong reliance on reactive technical aid instead of capacity building over the long term (EPA, 2024a; CRS, 2025). Reduced financial autonomy removes incentives to explore innovative modes of governance or human-focused resiliency initiatives, and this dependency on externally funded compliance operations is reaffirmed. Compared to that, the private utilities are allowed to re-invest in the process of continuous improvement and employee training, showing how investment asymmetry is turned into divergent cultural maturity (NASEO, 2020).

The most troublesome is the behavioral inertia. Organizational culture is a gradual process, especially within organizations that were historically inclined towards compliance. Research notes that in cases where the employees perceive cybersecurity as something that is imposed on them instead of a collective effort, the level of participation in prevention and reporting decreases (Willie, 2023; Said et al., 2022). Furthermore, leaders in the field of public utilities tend to assign cybersecurity to technical teams, undermining the apparent leadership endorsement that would support the culture (Georgiadou et al., 2022). Unless there is regular executive modeling, compliance frameworks do not infiltrate the behavioral layer that maintains preparedness. Consequently, the utilities are procedurally aligned and are susceptible to human-factor failures that cannot be guarded by any control checklist (Folorunso et al 2024).

6. POLICY AND MANAGERIAL IMPLICATIONS

The reviewed literature leads to a rather straightforward conclusion.Sustainable cybersecurity preparedness is based on policy frameworks that promote culture to the same extent as they impose regulations. This requires an adjustment of the regulative design, funding models, and measuring performance.

On the policy level, the agencies are becoming more aware of the necessity to incorporate culture metrics into the oversight programs. The leadership engagement, ongoing training, and information sharing are the measurable outcomes and the focus of the CISA Cybersecurity Performance Goals and Culture of Cyber Readiness initiative and are identified alongside technical controls (CISA, 2021, 2023). The 2024 guidance by EPA also proposes a change in the workforce-training expectations and executive-level accountability in compliance checklists, which is an indication of the transition to the behavior-based evaluation (EPA, 2024a). These changes explain how a hybrid form of regulation where compliance check and cultural evaluation support each other has emerged.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 1 | January 2026 - Peer Reviewed Journal

Policy tools which rely on incentives promote this change even more. The approvals of incentive-rate treatment of qualified cybersecurity investments issued by the FERC authority illustrate the ability of financial processes to encourage utilities that go beyond the minimum level of compliance (FERC, 2023a). These incentives promote active governance, which can drive innovation in the private sector and also get public utilities to embrace such performance-based models. Wider implementation of those mechanisms may turn the compliance requirements into development prospects, especially when combined with technical-assistance programs to address smaller utilities (NASEO, 2020).

As a manager, the readiness that requires incorporation of culture necessitates long-term leadership presence and interdisciplinary cooperation. Executives must position cybersecurity as an operating value in each process instead of a cost center in Information Technology (IT). Parallel advancements in integrated GIS, remote sensing, and machine learning for flood prediction demonstrate how utilities can adopt data-driven approaches to anticipate and mitigate environmental risks, reinforcing the need for holistic resilience strategies that combine cyber and physical dimensions (Gyang, Akomolafe, Panful, & Yowetu, 2025). The results of the empirical research prove that leadership modeling together with role-specific training and recognition increases compliance with secure behaviors significantly (Uchendu et al., 2021; Georgiadou et al., 2022). The experience of private utilities in implementing enterprise-wide awareness campaigns and certification programs can serve as a blueprint to the workforce engagement strategies that could be implemented by the public organizations (Martel et al., 2019). Such practices in the governance of a public sector, with the use of commonly available toolkits such as the CISA Implementation Action Checklist, would help to align behavioral readiness across utility types (EPA, 2024b).

Lastly, learning across sectors through the Internet of Things (IoT), sustainability, and smart city can be integrated to provide conceptual leverage by policymakers. These industries demonstrate how openness, collaboration among stakeholders, and trust of the population can help to speed up cultural adjustment to cybersecurity (Bonsu et al., 2025; Berlilana et al., 2021; Grigg, 2025). The ability to integrate such participatory models in utility governance can enhance not only cyber readiness but also confidence within society to resilience of critical infrastructure.

The aggregate evidence highlights the importance of the fact that compliance and culture are not contrary paradigms but phases of maturity. Compliance brings accountability at the baseline level, culture at the institutional level brings constant vigilance. Policymakers are faced with the challenge of creating regulatory ecosystems which cut across this continuum by coordinated regulation, fair distribution of resources, and behavioral incentives. The solution to these systemic and cultural gaps will be the future evolution of the governance of cybersecurity among utilities in the United States and make compliance a collective resiliency, rather than just adherence (Folorunso et al 2024; CISA, 2023; NASEO, 2020).

7. RECOMMENDATIONS

Integrate culture metrics in regulatory control:
Indicators of organizational culture, such as leadership engagement, workforce participation, and learning maturity need to be incorporated into compliance frameworks by federal and state agencies. By integrating these human-factor metrics with the current technical audits, it would minimize the difference between official conformance and real resilience (CISA, 2023; EPA, 2024a).

Reward proactive investment in cybersecurity
Utilization of incentives like incentive-rate mechanism on cybersecurity enhancements that is granted by FERC can also be used in rewarding utilities that will have proven to be ready to innovate more than the minimum standards. These mechanisms would encourage both the utilities and the public to consider culture building as a value creation exercise and no longer as a regulatory expense (FERC, 2023a; NASEO, 2020).

Develop cross-sector workforce programs
There should be an integrated national structure that fosters recurring training and exercises based on the scenario in the water, energy, and digital-infrastructure sectors. DOE, CISA, and Pacific Northwest National Laboratory (PNNL) resources give templates of capacity-building curriculum based on experiential learning and inter-utility collaboration (Whyatt et al., 2021; EPA, 2024b).

Require leaders to be accountable regarding cybersecurity achievements
Risk governance needs to be a formal responsibility of leadership that has readiness performance indicators. The requirement of executive participation in the audit criteria will provide the top to down modeling of security practices and cultural ownership throughout the organizational levels embedded (Uchendu et al., 2021; Georgiadou et al., 2022).

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 1 | January 2026 - Peer Reviewed Journal

Establish learning consortia between private and public utilities:
CISA and NARUC should support structured peer-learning between municipal utility networks and an investor-owned utility network to share best practices, simulation results and workforce strategies. This kind of cooperation may help decrease the level of maturity and enhance national level of behavioral readiness (NARUC, 2019; CISA, 2023).

Embed transparency and community participation in resiliency programs:
Utility cybersecurity should go beyond internal governance to outside inside governance (that is, to include public-trust mechanism). Smart-city and sustainability models teach us that effective risk communication and involvement of the stakeholders can enhance compliance credibility and cultural legitimacy (Grigg, 2025; Berlilana et al., 2021; Bonsu et al., 2025).

8. CONCLUSION

The analytical synthesis of the policy, technical and behavioral research confirms that cybersecurity readiness in the utilities of the United States is in the paradigm shift, that is, enforcement of compliance to culture institutionalization. Though there are mandatory frameworks including NERC CIP, EPA guidance and CISA performance goals, that have raised protections at the base level but have not brought about uniform adaptive resilience. Public utilities are stuck in accountability based on audit which is limited by the unavailability of resources and disjointed control. With more flexibility in investment and strategic freedom, private utilities have an easier time making cybersecurity a part of corporate governance, workforce motivation and innovation channels.

In both industries, the facts reveal that culture is the driving force that can change compliance to competence. The presence of leadership, lifelong learning and shared accountability transform regulatory intent into collective action, which allows the utilities to preempt and respond to emerging cyber threats. Incorporation of human factors in readiness systems via policy incentives, governance reform, and cross-utility co-operation comes out as the new frontier in critical infrastructure protection.

Finally, utility cybersecurity maturity in the U.S will be assessed not by the level of the standards achieved but by the extent to which secure behavior is the norm, leadership is resilient, and compliance is transforming into culture. This mixture will not be possible without coordinated policy design, distribution of available resources fairly, and sustained organizational learning, in this way, the readiness will not only be recorded on paper but also reflected in the everyday behavior of any utility professional.

REFERENCES

1. *Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization benefits as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. Sustainability, 13(24), 13761.*
2. *Bonsu, Mildred & Oware, Derrick & Donkor, Alice. (2025). The role of cybersecurity regulation, policy, and compliance in strengthening IoT security and reducing consumer risks. World Journal of Advanced Research and Reviews. 27. 2500-2507. 10.30574/wjarr.2025.27.1.2508.*
3. *CISA (2023). Cross-Sector Cybersecurity Performance Goals. PERFORMANCE GOALS Version: 1.0.1. https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf*
4. *CISA. (2021). Ongoing Cyber Threats to U.S. Water and Wastewater Systems. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a*
5. *CISA. (2025). Secure Your Business. Protect your business, employees and customers with smart cybersecurity practices. https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business*
6. *Congressional Research Service (CRS). (2025). Cybersecurity of the Municipal Water Sector: Background and Issues for Congress. https://www.everycrsreport.com/files/2025-06-03_R48556_cc4193c57e9e5c8f01239fcd63b0395eb39f24fb.pdf*
7. *Conway, T., Gutierrez, T., & Mathezer, S. (2024). How to Use NERC-CIP: An Overview of the Standards and Their Deployment with Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-sans-fortinet-nerc-cip-overview.pdf*
8. *DOE, U. (2022). Cybersecurity Considerations for Distributed Energy Resources on the US Electric Grid.*
9. *EPA (2024). EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems. EPA Office of Water (4608T). https://www.epa.gov/system/files/documents/2024-08/epa-guidance-on-improving-cybersecurity-at-drinking-water-and-wastewater-systems-1.pdf*
10. *EPA. (2024). Cyber Incidents at Water and Wastewater Utilities. Incident Action Checklist – Cybersecurity. Office of Water (4608-T). https://www.epa.gov/system/files/documents/2024-09/240909_cybersecurityiac_fillable_508c.pdf*
11. *Federal Energy Regulatory Commission (FERC). (2023). FERC Approves Incentive Rate Treatment for Cybersecurity Investments. Docket No. RM22-19-000. https://www.ferc.gov/news-events/news/ferc-approves-incentive-rate-treatment-cybersecurity-investments*
12. *Federal Energy Regulatory Commission (FERC). (2023). Incentives for Advanced Cybersecurity Investment. Federal Register/Vol. 88, No. 85. https://www.govinfo.gov/content/pkg/FR-2023-05-03/pdf/2023-08929.pdf*

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 1 | January 2026 - Peer Reviewed Journal

13. *Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). Security compliance and its implication for cybersecurity. World Journal of Advanced Research and Reviews, 24(01), 2105-2121.*
14. *Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. Journal of Computer Information Systems, 62(3), 452-462.*
15. *GOA, (2024) CRITICAL INFRASTRUCTURE PROTECTION EPA. Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems. https://www.gao.gov/assets/gao-24-106744.pdf*
16. *Grigg, N. S. (2025). Digital Transformation in Water Utilities: Status, Challenges, and Prospects. Smart Cities, 8(3), 99.*
17. *Gyang, P. A.-E., Akomolafe, O., Panful, B., & Yowetu, I. A. (2025). A review of integrated use of machine learning algorithms, GIS and remote sensing techniques in the prediction of rainfall patterns and floods in the U.S. World Journal of Advanced Engineering Technology and Sciences, 14(1), 159–167. https://doi.org/10.30574/wjaets.2025.14.1.0025*
18. *Lin, W. C., & Saebeler, D. (2019). Risk-based v. compliance-based utility cybersecurity-a false dichotomy. Energy LJ, 40, 243.*
19. *Martel, E., Kariger, R., & Graf, P. (2019). Cyber resilience in the electricity ecosystem: Principles and guidance for boards. Center for Cybersecurity and Electricity Industry Community*
20. *McCarthy, J., Stea, B., & Faatz, D. (2023). Cybersecurity for the water and wastewater sector: A practical reference design for mitigating cyber risk in water and wastewater systems.*
21. *Moore, C. (2015). NERC CIP Overview. Duke Energy, Center for Advanced Power Engineering Research. https://caper-usa.com/wp-content/uploads/2017/04/CIP-Overview.pdf*
22. *Moraitis, G., Sakki, G. K., Karavokiros, G., Nikolopoulos, D., Tsoukalas, I., Kossieris, P., & Makropoulos, C. (2023). Exploring the cyber-physical threat landscape of water systems: a socio-Technical modelling approach. Water, 15(9), 1687.*
23. *NASEO. (2020). Enhancing Energy Sector Cybersecurity: Pathways for State and Territory Energy Offices. https://www.naseo.org/data/sites/1/documents/publications/Final%20NASEO_Cybersecurity%20Report%20%28062020%29.pdf*
24. *National Association of Regulatory Utility Commissioners (NARUC). (2019). Essential Guide to NARUC Cybersecurity Resources. https://pubs.naruc.org/pub/403C8E5A-99E0-B07E-7A13-6817D9CCFC95*
25. *NIST, (2024) The NIST Cybersecurity Framework (CSF) 2.0 https://doi.org/10.6028/NIST.CSWP.29*
26. *Onyekwuluje, T. P., Akoto-Bamfo, D., Tetteh-Kpakpah, C., Panful, B., & Oware, D. (2025). Evaluating the role of cybersecurity audits in protecting the U.S. capital market. **World** Journal of Advanced Research and Reviews, 25(2), 974–980. https://doi.org/10.30574/wjarr.2025.25.2.0183*
27. *Panful, B., Apaflo, B., & Hutchful, N. (2025). Cyber-Physical Systems Under Threat: A Case-Study Review of Recent SCADA Attacks in the U.S. Utility Sector. Sarcouncil Journal of Engineering and Computer Sciences, 4(12), 104–117. https://doi.org/10.5281/zenodo.18030630*
28. *Panful, B., Apaflo, B., Filani, A., Nnadi, K., & Hutchful, N. (2025). Human factor vulnerabilities in energy industry cybersecurity: Assessing employee awareness and behavior in breach prevention. International Journal for Multidisciplinary Research, 7(6), 1–XX.*
29. *Said, N. S. M., Yusof, R., Ali, S. R. O., Mat, K. A., & Mansor, F. A. (2022). Employees' Performance and Organisational Culture in the Utility Sector. Jurnal Intelek, 17(1), 246-256.*
30. *Souppaya, M., Scarfone, K., & Dodson, D. (2022). Secure software development framework (ssdf) version 1.1. NIST Special Publication, 800(218), 800-218.*
31. *Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387.*
32. *Whyatt, M. V., Thorsen, D. E., Powers, F. E., Watson, M. A., McKinnon, A. D., & Seaman, J. D. (2021). Department of Energy Water Power Technologies Office Cyber Response & Recovery Flipbook [Slides] (No. PNNL-30538). Pacific Northwest National Lab.(PNNL), Richland, WA (United States).*
33. *Willie, M. M. (2023). The role of organizational culture in cybersecurity: building a security-first culture. Journal of Research, Innovation and Technologies, 2(2 (4)), 179-198.*