International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Standardized Cybersecurity Assessments as Governance Instruments Across Critical Infrastructure Sectors

Dr. Robb Shawe (Lead Author)
Dr. Gilbert B. Mengnjo (Co-Author)

Capitol Technology University, Department of Critical Infrastructure
11301 Springfield Road, Laurel, MD 20708, USA

doi.org/10.51505/ijaemr.2026.11202 URL: http://dx.doi.org/10.51505/ijaemr.2026.11202

Received: Feb 21, 2026 Accepted: Mar 02, 2026 Online Published: Mar 09, 2026

Abstract
Standardized cybersecurity assessments are widely used across critical infrastructure sectors to evaluate security posture, demonstrate regulatory alignment, and identify control gaps. However, assessments are often treated as technical checklists or compliance artifacts, which limits their value for governance, oversight, and strategic decision-making. This article argues that standardized cybersecurity assessments—when aligned with governance frameworks and maturity models—function most effectively as governance instruments rather than static diagnostic tools. Using healthcare supply chain cybersecurity and energy infrastructure governance as illustrative contexts, the article shows how assessment outputs can improve leadership visibility, cross-unit comparability, prioritization, and accountability. By reframing cybersecurity assessments as governance-enabling mechanisms, this study contributes to the literature on cybersecurity governance and critical infrastructure protection while offering practical guidance for executives, boards, and policymakers responsible for systemic resilience and cyber risk oversight.

Keywords: NIST Cybersecurity Framework (CSF) 2.0; Cybersecurity Capability Maturity Model (C2M2); Cyber Security Evaluation Tool (CSET); cybersecurity governance; critical infrastructure protection; supply chain cybersecurity; resilience; enterprise risk management

1. Introduction

Cybersecurity risk in critical infrastructure environments has evolved beyond isolated information systems. Modern infrastructures are characterized by extensive interdependencies among operational technology (OT), information technology (IT), cloud platforms, managed service providers, and complex supply chains. In this context, cybersecurity failures rarely remain localized; instead, they propagate across organizational, sectoral, and geographic boundaries, amplifying operational and societal consequences.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

In this article, the term cybersecurity assessment outputs refers to the structured findings generated by standardized cybersecurity assessment instruments, including maturity model results, domain scores, and governance-relevant evidence artifacts. In response to this complexity, organizations increasingly rely on standardized cybersecurity assessments to evaluate security posture, benchmark maturity, and demonstrate alignment with regulatory and industry expectations. Frameworks and tools aligned with the National Institute of Standards and Technology (NIST) provide widely adopted guidance for cybersecurity risk management and governance across critical infrastructure sectors. The NIST Cybersecurity Framework (CSF) 2.0 organizes cybersecurity outcomes and introduces an explicit governance function that supports enterprise risk decisions (NIST, 2024). The Cybersecurity Capability Maturity Model (C2M2) provides a maturity-based structure for evaluating and improving cybersecurity capabilities across organizational domains (U.S. Department of Energy [DOE], 2022). The Cyber Security Evaluation Tool (CSET®) provides a structured, repeatable assessment workflow widely used across industrial and critical infrastructure environments (Cybersecurity and Infrastructure Security Agency [CISA], 2024). However, despite their ubiquity, assessment results are often treated as technical artifacts or compliance checklists rather than as inputs to governance and strategic decision-making.

This narrow interpretation limits the value of assessment activities. Summary scores, heat maps, and control-level findings frequently fail to communicate risk in ways that support executive prioritization, board oversight, or enterprise risk management. As a result, organizations may appear compliant while remaining vulnerable to systemic cyber risks driven by uneven capabilities, fragmented governance, and unaddressed interdependencies.

This article argues that standardized cybersecurity assessments function most effectively when understood and applied as **governance instruments**. When interpreted beyond compliance and integrated into leadership and oversight processes, assessment outputs can illuminate systemic risk, reveal cross-unit variability, and support evidence-based governance decisions. Drawing on doctoral research in healthcare supply chain cybersecurity and energy infrastructure governance, this study reframes cybersecurity assessments as mechanisms that translate technical measurement into actionable governance insight across critical infrastructure sectors.

In this article, the term standardized cybersecurity assessment refers to structured, repeatable instruments—questionnaires, rubrics, or tool-based evaluations—used to measure control implementation and capability against a defined reference model. The governance claim advanced here is that the primary value of such assessments lies not in the score itself, but in the governance signal produced when results are made comparable across units, time, and dependencies. Furthermore, this analysis forms part of a broader, multi-article research program examining the governance and interpretation of cybersecurity assessment outputs across critical infrastructure contexts (Shawe, 2026).

Vol. 11, No. 02; 2026

ISSN: 2456-3676

This manuscript constitutes a segment of a comprehensive research initiative exploring the governance interpretation of cybersecurity assessment results within critical infrastructure contexts. The series examines how cybersecurity assessments, maturity models, and governance frameworks affect organizational learning, risk-management prioritization, and resilience in complex socio-technical systems. By integrating multidisciplinary academic analysis with practitioner perspectives, the research aims to elucidate how governance structures, regulatory environments, and organizational accountability influence the efficacy of cybersecurity risk management and operational resilience.

1.1 Methodological Orientation

This study adopts a qualitative conceptual analysis of governance. Rather than collecting primary empirical data, the article synthesizes established cybersecurity assessment frameworks, governance theory, and critical infrastructure scholarship to examine how standardized cybersecurity assessment outputs function as governance instruments. The analysis is comparative and interpretive, drawing on healthcare supply chain and energy infrastructure contexts as illustrative domains rather than as empirical case studies.

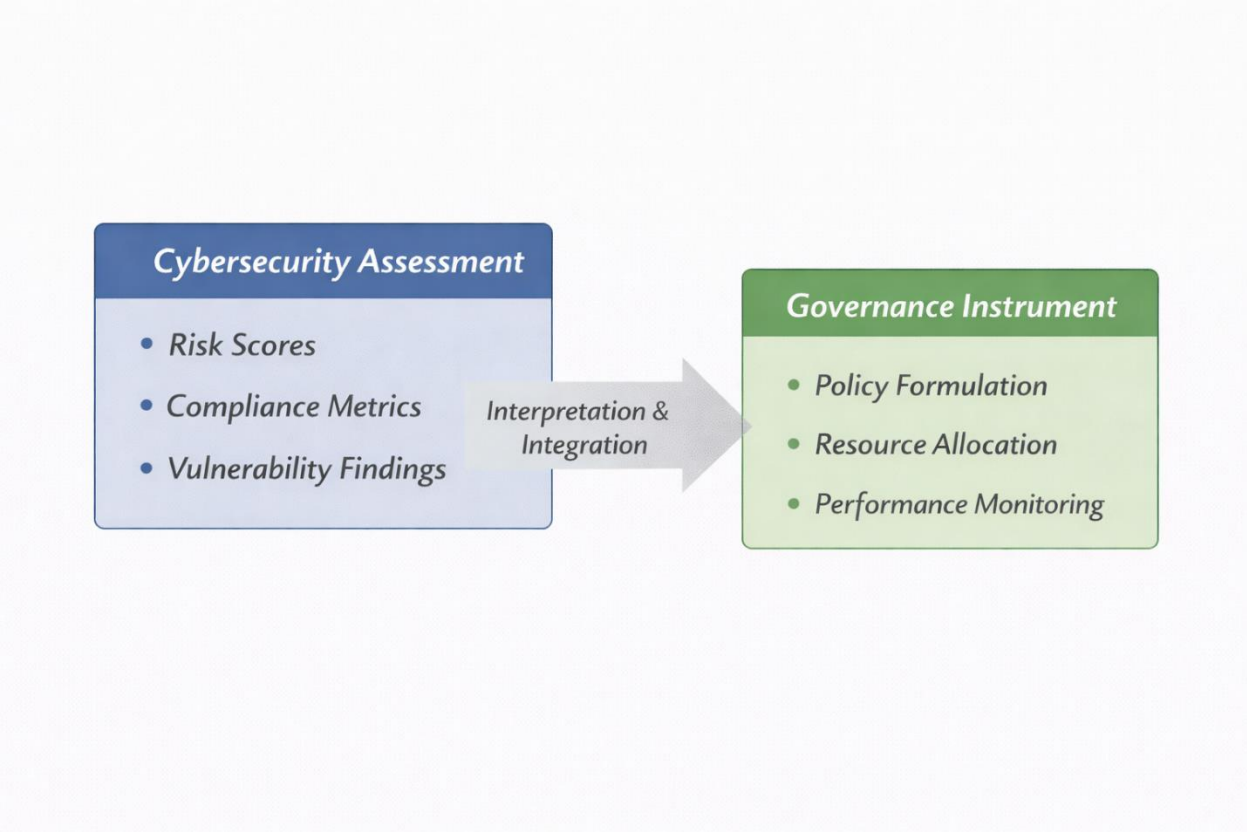
The methodological approach emphasizes the integration of theory, boundary analysis, and governance reframing. The objective is not to establish causal generalization but to clarify how assessment outputs acquire governance meaning when embedded within leadership oversight structures, decision-rights allocation, and accountability mechanisms. This conceptual orientation aligns with established traditions in governance scholarship that seek to reframe instruments and structures without requiring primary field data. To clarify how standardized cybersecurity assessments can shift from compliance-oriented artifacts to governance-enabling instruments, the conceptual transformation described in this study is illustrated in Figure 1.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Figure 1

Compliance-Oriented vs. Resilience-Oriented Interpretation of Cybersecurity Maturity Models



Note. Author created. The figure illustrates the conceptual transformation of standardized cybersecurity assessment outputs into governance instruments. Assessment outputs (e.g., risk scores, compliance metrics, vulnerability findings) generate governance value when interpreted and integrated within leadership oversight structures, enabling policy formulation, resource allocation, and performance monitoring. The model is conceptual and synthesizes governance theory, maturity modeling, and structured assessment practices discussed in this study.

The governance transformation mechanism described in this study is illustrated in Figure 1.

2. Governance and Cybersecurity in Critical Infrastructure

Cybersecurity governance refers to the structures, processes, decision rights, and information flows through which organizations direct, monitor, and evaluate cybersecurity activities in alignment with mission objectives and risk appetite. In critical infrastructure sectors, governance challenges are intensified by regulatory complexity, distributed ownership, and the convergence of IT and OT environments. Governance-oriented standards such as ISO/IEC 27014 emphasize leadership direction, organizational alignment, and performance monitoring as prerequisites for effective information security governance (ISO/IEC, 2020).

Vol. 11, No. 02; 2026

ISSN: 2456-3676

CSF 2.0 explicitly positions cybersecurity as an enterprise risk management concern, emphasizing outcomes that support understanding, assessment, prioritization, and communication of cyber risk (NIST, 2024). This governance orientation reflects a broader shift away from prescriptive controls toward outcome-based risk management. However, outcome-based frameworks require mechanisms that allow leaders to evaluate progress and compare performance across organizational units and over time.

Doctoral research in healthcare supply chain cybersecurity highlights that governance gaps often arise not from a lack of policy intent but from insufficient measurement and inconsistent oversight. Boards and executive leaders may lack standardized indicators to compare cybersecurity capabilities across units, vendors, or operational contexts. Without such indicators, governance becomes reactive and fragmented.

Similarly, energy infrastructure governance operates across multiple organizations and regulatory regimes, making consistent oversight difficult. In these environments, governance effectiveness depends on the availability of structured, comparable information that can support coordination, prioritization, and accountability across boundaries.

Standardized cybersecurity assessments provide a mechanism to address these governance challenges—if they are designed and interpreted with governance needs in mind.

3. From Compliance Tools to Governance Instruments

Historically, cybersecurity assessments have been closely associated with compliance verification. Organizations complete assessments to demonstrate alignment with standards, satisfy auditors, or meet regulatory expectations. While this function remains essential, it represents only a subset of the potential value of assessment outputs.

When assessments are treated solely as compliance tools, their outputs are often reduced to binary pass/fail judgments or aggregated scores that obscure underlying variability. Such representations provide limited insight into systemic risk, particularly in environments characterized by interdependence and uneven capability.

Reframing assessments as governance instruments requires a shift in purpose and interpretation. As governance instruments, assessments are valued for their ability to:

- Provide **comparability** across organizational units and time,
- Reveal **distribution of risk**, not merely average posture,
- Support **prioritization** of resources and interventions,
- Enable **accountability** through repeatable measurement.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

This reframing aligns cybersecurity assessment with established governance practices in other risk domains, in which measurement informs strategic oversight rather than demonstrating compliance.

4. Maturity Models and Governance Visibility

Maturity models play a critical role in translating governance intent into measurable capability. Unlike checklist-based assessments, maturity models describe a staged progression, enabling organizations to evaluate not only whether practices exist but also how effectively they are institutionalized and sustained.

The Cybersecurity Capability Maturity Model (C2M2) exemplifies this approach. Designed for critical infrastructure environments, C2M2 provides a structured self-evaluation methodology that spans IT and OT domains and organizes practices into maturity indicator levels (MILs) that support capability progression (DOE, 2022). Its emphasis on progression supports governance functions by enabling leaders to:

- Assess current-state capability,
- Define target maturity levels aligned with risk tolerance,
- Track improvement over time.

Doctoral research in energy infrastructure governance demonstrates that maturity-based reporting is more intelligible to executives and policymakers than technical control inventories. Maturity levels provide a shared language that facilitates communication between technical specialists and governance bodies.

However, maturity models alone are insufficient. They require structured assessment mechanisms to generate reliable data and ensure consistency across units and contexts.

5. Structured Assessment as an Operational Mechanism

Structured assessment tools operationalize governance and maturity concepts by providing disciplined, repeatable evaluation processes. Tools such as the Cybersecurity Evaluation Tool (CSET) exemplify this role in critical-infrastructure contexts, particularly when industrial control systems are involved.

CSET is designed to guide organizations through a systematic evaluation of cybersecurity practices in accordance with recognized standards and guidance. Its structured questionnaires and reporting outputs support repeatability, benchmarking, and trend analysis—features that are essential for governance use (CISA, 2024).

From a governance perspective, structured assessment tools serve as the **operational bridge** between high-level frameworks and day-to-day practice. They enable organizations to:

- Baseline performance consistently,

Vol. 11, No. 02; 2026

ISSN: 2456-3676

- Identify gaps relative to target maturity,
- Produce evidence suitable for executive reporting and oversight.

Doctoral research in healthcare supply chain environments shows that such structured assessments are particularly valuable for exposing cross-unit variability that would otherwise remain hidden behind enterprise-level compliance claims.

6. Illustrative Sector Contexts

6.1 Healthcare Supply Chain Cybersecurity

Healthcare supply chains are characterized by extensive reliance on third-party vendors, distributed clinical environments, and varying cybersecurity capabilities. Assessments conducted at the unit or vendor level frequently reveal uneven monitoring practices, inconsistent documentation, and fragmented accountability.

When interpreted through a governance lens, these assessment outputs provide insight into systemic risk rather than isolated deficiencies. Governance bodies can use assessment data to identify where supply chain dependencies introduce disproportionate exposure and where targeted interventions are necessary.

This illustrates the governance value of aggregated and contextualized assessment outputs, rather than treating them as isolated technical findings.

6.2 Energy and Smart Grid Infrastructure

Energy infrastructure governance spans utilities, regulators, vendors, and public authorities. In this environment, cybersecurity assessments and maturity evaluations support coordination across organizational boundaries.

Doctoral research in this sector demonstrates that assessment outputs aligned with maturity models can inform policy alignment, investment prioritization, and resilience planning. Governance value increases when assessments are interpreted longitudinally, supporting trend analysis and strategic planning rather than one-time compliance verification.

7. Cross-Sector Synthesis

Across healthcare and energy sectors, a consistent pattern emerges: standardized cybersecurity assessments generate governance value when they are aligned with frameworks, interpreted through maturity models, and integrated into oversight processes.

Key governance insights include:

- **Variability matters:** Average scores obscure risk distribution.
- **Comparability enables oversight:** Standardization supports accountability.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

- **Measurement supports action:** Governance improves when assessment results inform prioritization and resource allocation.

These insights suggest that assessment processes should be explicitly designed to support governance objectives rather than merely to evaluate technical performance.

8. Implications for Governance Practice

For executives, boards, and policymakers, the findings of this study suggest several practical implications:

1. Cybersecurity assessments should be selected and designed with governance use in mind.
2. Assessment outputs should be translated into maturity-based and risk-distribution narratives suitable for leadership oversight.
3. Governance processes should incorporate assessment results into enterprise risk management and strategic planning cycles, including risk register and portfolio discussions that connect cybersecurity measurement to enterprise risk decisions (Quinn et al., 2021; Quinn et al., 2025).

By adopting this approach, organizations can move from symbolic compliance toward evidence-based cyber risk governance.

9. Significance and Contribution

This article contributes to the cybersecurity governance literature by reconceptualizing standardized assessments as governance instruments rather than technical checklists. It integrates governance theory, maturity modeling, and structured assessment into a coherent framework applicable across critical infrastructure sectors.

In practice, it provides leaders with a defensible approach to translating cybersecurity measurements into oversight and accountability. Conceptually, it advances understanding of how assessment mechanisms shape the effectiveness of governance in complex socio-technical systems.

10. Limitations and Boundary Conditions

This analysis is conceptual and does not rely on primary empirical case studies or quantitative testing. As a result, findings are interpretive rather than generalizable. The healthcare and energy sectors serve as illustrative contexts, and conclusions should not be assumed to apply uniformly across all critical infrastructure environments without contextual adaptation.

Future research may extend this work through empirical investigation, including case-based validation, interview-based governance analysis, or longitudinal examination of assessment-driven decision-making processes. Nonetheless, the conceptual reframing offered here provides a foundation for such inquiry and clarifies governance mechanisms that empirical research may further examine.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

11. Conclusion

Standardized cybersecurity assessments are necessary but insufficient when treated solely as compliance mechanisms. When reframed as governance instruments, assessment outputs become critical infrastructure for decision-making, oversight, and resilience planning. Aligning frameworks, maturity models, and structured assessment tools enables organizations to transform cybersecurity measurement into meaningful governance action, thereby strengthening resilience across critical infrastructure systems.

Authorship Statement

Dr. Robb Shawe and Dr. Gilbert Mengnjo jointly conceptualized the research orientation and governance perspective of this manuscript. Dr. Mengnjo contributed practitioner expertise spanning more than 15 years in cybersecurity governance, enterprise risk management, regulatory compliance, and healthcare information security.

Dr. Shawe contributed a multidisciplinary scholarly synthesis integrating critical infrastructure protection, cybersecurity governance, organizational resilience, and socio-technical systems theory. Dr. Shawe also led the development of the conceptual framing, literature integration, and manuscript preparation.

Both authors collaborated in refining the analytical framework, reviewing the manuscript, and approving the final version for submission.

This manuscript forms part of a broader **scholarly program of research** examining cybersecurity governance, risk management maturity, and resilience across critical infrastructure and organizational ecosystems.

Author Note and Copyright Statement

Dr. Robb Shawe, PhD, MS

Dr. Robb Shawe is a scholar-practitioner, U.S. Navy veteran, and Chief Executive Officer of New York Security Consulting Professionals L.L.C. His research focuses on critical infrastructure protection, cybersecurity governance, organizational resilience, and socio-technical risk management. His scholarship integrates multidisciplinary perspectives spanning cybersecurity, emergency management, occupational health, and sustainability systems.

Dr. Shawe served as the lead author and was primarily responsible for conceptualization, development of the analytical framework, literature synthesis, and manuscript preparation. His

Vol. 11, No. 02; 2026

ISSN: 2456-3676

work emphasizes the integration of governance structures, resilience systems, and policy frameworks designed to strengthen critical infrastructure and organizational security environments.

Dr. Gilbert Mengnjo, PhD, MSc

Dr. Gilbert Mengnjo is a cybersecurity governance strategist and risk management leader with more than 15 years of experience guiding enterprise cybersecurity programs across healthcare, manufacturing, global supply chains, and critical infrastructure environments. His expertise includes cybersecurity governance, regulatory compliance, vendor risk management, and security program development aligned with frameworks such as NIST CSF, HIPAA, HITRUST, and ISO 27001.

Dr. Mengnjo contributed practitioner insights, governance analysis, and applied cybersecurity expertise to the conceptual development of the research framework and literature synthesis. His experience translating complex technical risks into operational governance strategies informed the manuscript's analytical perspective.

Conflict of Interest Statement

The authors declare no conflicts of interest related to this research.

Originality Statement

This manuscript represents original scholarly work and is not currently under consideration by another publication outlet.

Copyright Notice

References

Boyens, J. M., Paulsen, C., Bartol, N., Winkler, K., & Gabel, O. (2022). Cybersecurity supply chain risk management practices for systems and organizations (NIST SP 800-161 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Cybersecurity and Infrastructure Security Agency. (2024). Cyber Security Evaluation Tool (CSET®). U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset

Department of Energy. (2022). Cybersecurity Capability Maturity Model (C2M2) Version 2.1. U.S. Department of Energy. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

ISO/IEC. (2020). ISO/IEC 27014:2020—Information security, cybersecurity and privacy protection — Governance of information security. International Organization for Standardization.

Joint Task Force. (2018). Risk Management Framework for information systems and organizations: A system life cycle approach for security and privacy (NIST SP 800-37 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

Mengnjo, G. B. (2026). Assessing healthcare supply chain cybersecurity using the Cyber Security Evaluation Tool (CSET) (Unpublished doctoral dissertation). Capitol Technology University.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Quinn, S., Ivy, N., Barrett, M., & Witte, G. (2021). Identifying and estimating cybersecurity risk for enterprise risk management (NIST IR 8286A). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8286A.pdf

Quinn, S., Ivy, N., Barrett, M., Witte, G., Gardner, R., & Smith, M. (2025). Prioritizing cybersecurity risk for enterprise risk management (NIST IR 8286B-upd1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8286B-upd1.pdf

Shawe, R. (2025). *Exploring smart grid technologies' impact on sustainable energy management in New York State* (Publication No. 32284053) [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations & Theses Global.

This manuscript forms part of a coordinated research program examining cybersecurity assessment governance; related manuscripts address distinct research questions and are submitted to separate journals or editorial tracks.