International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

When Cybersecurity Assessment Fails to Reduce Risk: Assessment Fatigue and Governance Design

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.2026.11210 URL: http://dx.doi.org/10.51505/ijaemr.2026.11210

Received: Mar 06, 2026 Accepted: Mar 17, 2026 Online Published: Mar 24, 2026

Abstract

Cybersecurity assessments have become a routine feature of risk management in critical infrastructure organizations. Maturity models, compliance audits, and structured evaluations are widely used to demonstrate due diligence and inform decision-making. Despite this extensive assessment activity, many organizations continue to experience significant cyber incidents, raising questions about the effectiveness of assessment-driven security strategies. This qualitative, conceptual analysis examines the phenomenon of assessment fatigue and explores the governance conditions under which cybersecurity assessment fails to produce meaningful risk reduction. Rather than attributing failure to assessment quality or frequency alone, the article argues that governance design determines whether assessment findings translate into action. Drawing on perspectives on governance effectiveness, symbolic compliance, and organizational learning, the study explains how assessment can become performative rather than corrective. The article concludes by identifying governance conditions under which assessment activity contributes to absolute risk reduction and organizational resilience.

Keywords: Cybersecurity assessment; assessment fatigue; governance design; symbolic compliance; organizational learning; critical infrastructure; risk reduction

1. Introduction

Cybersecurity assessments are now ubiquitous across critical infrastructure sectors. Organizations routinely conduct maturity assessments, compliance audits, and third-party evaluations to measure cyber posture, satisfy regulatory expectations, and inform leadership oversight (Cybersecurity and Infrastructure Security Agency [CISA], 2024; National Institute of Standards and Technology [NIST], 2024).

Despite this proliferation of assessment activity, cyber incidents continue to disrupt healthcare systems, energy infrastructure, and other critical services. In many cases, organizations that experience significant cyber events have completed multiple assessments prior to the incident.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

This disconnect raises an important governance question: why do **repetitive evaluation cycles** so often fail to reduce cyber risk?

One emerging explanation is **assessment fatigue**—a condition in which organizations continue to perform assessments without achieving corresponding improvements in security outcomes. Assessment fatigue is not merely a matter of workload or repetition; it reflects deeper governance dynamics that shape how assessment findings are interpreted, prioritized, and acted upon. Moreover, this article examines the governance conditions under which cybersecurity assessments fail to produce meaningful risk reduction. It argues that assessment failure is rarely due to a lack of information and more often to governance designs that inhibit learning, accountability, and corrective action.

The manuscript constitutes a segment of an extensive research initiative exploring the interpretation of governance in cybersecurity assessment results within critical infrastructure sectors. The series aims to examine how cybersecurity evaluations, maturity models, and governance frameworks affect organizational learning, risk management priorities, and resilience in complex socio-technical systems. By integrating interdisciplinary academic insights with practitioner-informed perspectives, the research endeavors to elucidate how governance structures, regulatory environments, and organizational accountability influence the effectiveness of cybersecurity risk management and operational resilience.

Furthermore, this study extends existing cybersecurity governance literature by focusing specifically on the governance conditions that determine whether assessment outputs translate into meaningful risk reduction. Unlike prior work that emphasizes assessment frameworks, reporting mechanisms, or technical control evaluation, this analysis centers on governance design as the primary determinant of assessment effectiveness. By conceptualizing cybersecurity assessments as governance signals rather than purely technical instruments, the study introduces a translation-focused governance perspective that distinguishes between performative assessment activity and corrective, outcome-driven security practices.

1.1 Methodological Orientation

This article adopts a qualitative, comparative governance analysis examining how cybersecurity assessment models are interpreted across healthcare and energy infrastructure contexts. Rather than evaluating the sufficiency of technical controls, the analysis focuses on the sector's mission, governance structure, regulatory context, and prioritization of consequences as determinants of assessment meaning. The approach is conceptual and comparative rather than empirical.

Conceptual governance analysis is particularly appropriate for examining cybersecurity assessment fatigue because the phenomenon involves organizational interpretation, decision authority, and institutional learning processes rather than technical control implementation alone. By synthesizing insights from governance effectiveness theory, symbolic compliance literature, and organizational learning research, the analysis develops an explanatory framework for

Vol. 11, No. 02; 2026

ISSN: 2456-3676

understanding why assessment activity may fail to produce risk reduction even when technical evaluation processes are robust.

2. Background and Context

2.1 Proliferation of cybersecurity assessments

In this article, the term cybersecurity assessment outputs refers to the structured findings generated by standardized cybersecurity assessment instruments. Cybersecurity assessments have expanded rapidly as organizations seek structured ways to evaluate risk and demonstrate due diligence. As a result, organizations may conduct multiple overlapping evaluations annually—internal audits, external reviews, maturity evaluations, and sector-specific exercises—often using similar criteria.

2.2 Critiques of checklist-based security

Prior research has criticized checklist-based approaches to cybersecurity for emphasizing the presence of controls over effectiveness and context. While checklists provide structure, they may encourage compliance behaviors rather than adaptive security practices (Stine et al., 2020).

2.3 Organizational fatigue and symbolic compliance

Organizational studies describe **symbolic compliance** as a condition in which organizations adopt formal processes to signal legitimacy without substantively changing behavior. When evaluations are decoupled from action, they risk becoming symbolic artifacts rather than instruments of improvement.

2.4 Gap in existing explanations

While technical and operational critiques of assessment limitations exist, fewer analyses examine assessment failure through a governance lens. Specifically, limited attention has been given to how governance design shapes whether assessment findings lead to learning and risk reduction. 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).

3. Problem Statement

It is unclear why repeated cybersecurity assessments often fail to yield meaningful risk reduction in critical infrastructure organizations.

As a result, organizations may accumulate assessment outputs without achieving improved resilience, while governance bodies mistakenly equate assessment activity with risk management effectiveness.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

4. Purpose of the Study

The purpose of this qualitative, conceptual analysis is to examine how governance design influences whether cybersecurity assessment activities lead to meaningful risk reduction in critical infrastructure organizations.

The study focuses on governance structures, accountability mechanisms, and learning processes rather than assessment methodologies or technical controls.

5. Research Questions

RQ1: How do critical infrastructure organizations experience cybersecurity assessment fatigue?

RQ2: What governance structures inhibit action on cybersecurity assessment findings?

RQ3: Under what governance conditions does assessment activity generate absolute risk reduction?

6. Theoretical and Conceptual Framework

This analysis integrates three complementary perspectives.
Governance effectiveness theory emphasizes the alignment of authority, accountability, and decision-making. Effective governance ensures that identified risks are owned and acted upon.
Symbolic compliance theory explains how organizations may adopt formal assessment practices to satisfy external expectations while avoiding substantive change.

Organizational learning theory focuses on the processes by which organizations convert information into adaptive behavior. Learning fails when feedback is not integrated into decision-making structures.

Together, these perspectives explain why assessment activity alone does not guarantee risk reduction and why governance design determines assessment effectiveness.

Table 1 summarizes the governance conditions that influence whether cybersecurity assessment activities lead to meaningful risk reduction or contribute to assessment fatigue.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Table 1

Governance Conditions Influencing Cybersecurity Assessment Effectiveness

Control Area	Healthcare (Patient Safety Lens)	Energy (Grid Stability Lens)
Incident Response	Focus on continuity of care and patient safety outcomes	Focus on grid continuity and the prevention of service disruption
Access Control	Protection of patient data and clinical systems	Protection of operational technology (OT) and control systems
System Availability	Ensuring uninterrupted clinical operations	Maintaining continuous energy generation and distribution
Risk Prioritization	Clinical impact and regulatory compliance (HIPAA)	Operational resilience and national infrastructure protection
Governance Focus	Patient safety, privacy, and care delivery	Infrastructure resilience, reliability, and cascading failure prevention

Note. Author created. The table summarizes governance conditions that determine whether cybersecurity assessment activities contribute to meaningful risk reduction or lead to assessment fatigue.

The governance conditions summarized in Table 1 illustrate that assessment effectiveness depends less on the technical design of evaluation tools and more on how organizations structure accountability and decision authority around assessment findings, with effective cybersecurity assessment ultimately determined by the alignment of governance authority, accountability, and action pathways that enable findings to translate into measurable risk reduction.

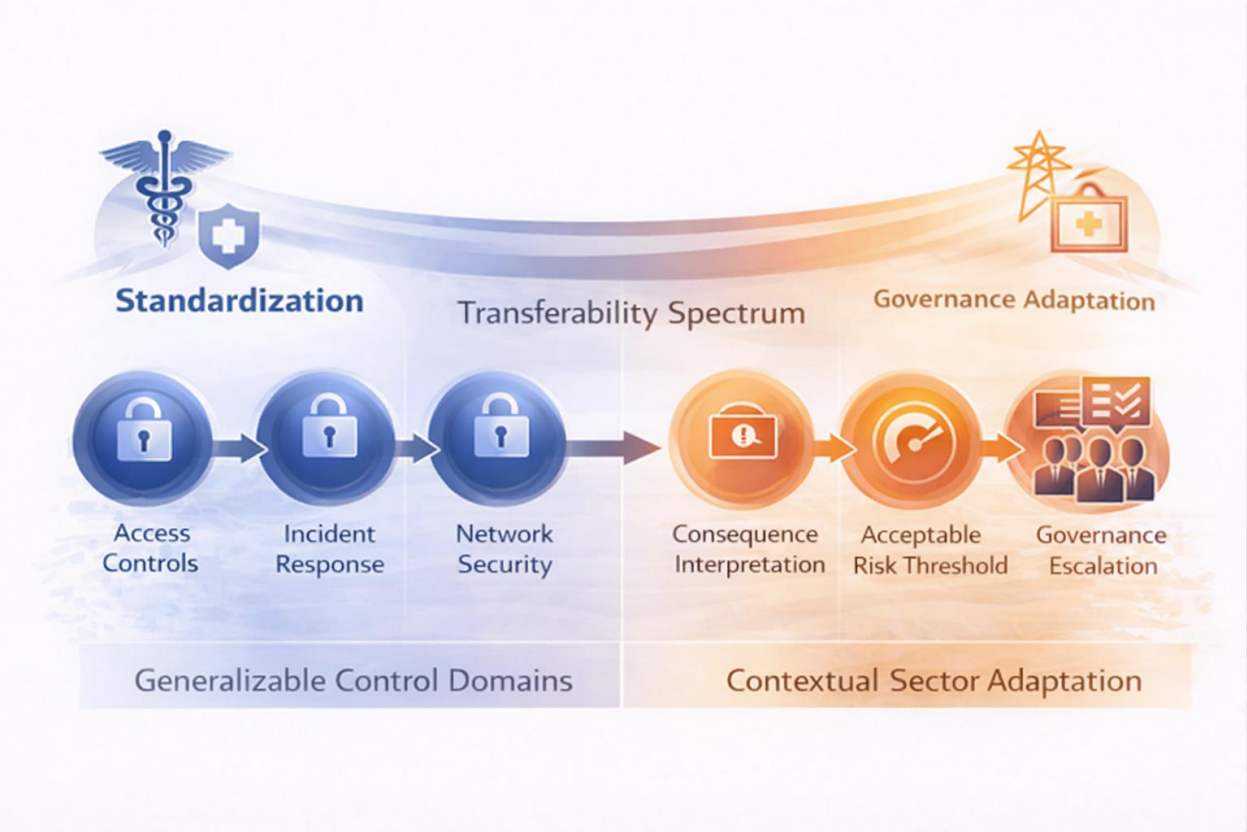
As illustrated in Figure 1, assessment transferability lies along a spectrum, with certain technical domains remaining stable across sectors while governance interpretation and consequence prioritization require contextual adaptation.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Figure 1

Assessment Transferability Spectrum Across Critical Infrastructure Sectors



Note. Author created. The figure illustrates a conceptual spectrum of the transferability of cybersecurity assessments across critical infrastructure sectors. Foundational control domains exhibit high generalizability, while consequence interpretation, acceptable risk thresholds, and governance escalation mechanisms require contextual adaptation. The model depicts transferability as contingent on governance alignment rather than as an inherent property of assessment instruments.

Figure 1 illustrates the spectrum of cybersecurity assessment transferability across critical infrastructure sectors, highlighting the distinction between stable technical domains and governance-dependent interpretation and prioritization of consequences. Taken together, this spectrum demonstrates that the effectiveness of cybersecurity assessment depends on governance alignment that translates standardized evaluation outputs into context-specific decision-making and risk prioritization.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

7. Assessment Fatigue as a Governance Outcome

Assessment fatigue emerges when organizations repeatedly identify similar gaps without resolving them. Findings are documented, reported, and archived, but responsibility for remediation remains unclear or contested.

Governance structures that diffuse accountability exacerbate this condition. Assessment fatigue is therefore not a failure of assessment tools but a predictable outcome of governance designs that prioritize reporting over action. When no single authority owns assessment outcomes, findings lose urgency and become normalized. Over time, assessments are perceived as administrative obligations rather than catalysts for change.

A practical illustration can be observed in healthcare organizations that repeatedly conduct cybersecurity maturity assessments aligned with frameworks such as NIST CSF or CISA CSET. Assessment outputs often identify deficiencies in asset visibility, incident-response coordination, and vendor-risk monitoring. Although these findings are documented and presented to leadership, responsibility for remediation may remain distributed among IT operations, compliance offices, and external vendors. Without clear governance and ownership, the same deficiencies may appear in subsequent assessments. In such cases, the assessment activity continues while corrective action stalls, reinforcing assessment fatigue.

8. Significance of the Study

This study explains why a cybersecurity assessment alone is insufficient for risk reduction. It shifts attention from assessment frequency and sophistication to governance design and accountability.

For practitioners, the analysis highlights the need to align assessments with decision authority and remediation ownership. For leaders and boards, it underscores the risk of equating assessment volume with security effectiveness. For policymakers, it suggests that mandating assessments without governance requirements may yield limited benefits.

9. Implications for Governance and Practice

To avoid **evaluation saturation**, organizations must redesign governance structures to ensure that assessment findings trigger action. This includes:

- Clear ownership of assessment outcomes
- Prioritization mechanisms aligned with risk appetite
- Integration of findings into enterprise risk and resilience decisions
- Accountability for remediation progress

Organizations implementing governance-centered assessment practices may encounter several institutional challenges. Resource constraints, competing operational priorities, and organizational resistance to accountability can limit the effectiveness of assessment-driven

Vol. 11, No. 02; 2026

ISSN: 2456-3676

remediation efforts. In addition, governing boards may lack the technical literacy necessary to interpret cybersecurity risk signals, creating communication barriers between technical specialists and decision-makers. Addressing these challenges requires stronger translation mechanisms, clearer accountability structures, and sustained leadership engagement.

When governance structures support learning and accountability, assessments can become powerful tools for continuous improvement rather than symbolic exercises (Stine et al., 2020; Shawe, 2026).

Without such translation, assessment outputs risk functioning as governance artifacts that signal diligence without enabling decision accountability.

10. Limitations and Future Research

This study is conceptual and does not present empirical data. Future research should examine assessment fatigue through case studies, governance audits, and longitudinal analysis of assessment-to-action pathways across critical infrastructure sectors.

11. Conclusion

Cybersecurity assessments are widely used, yet cyber risk persists. This paradox reflects governance failure rather than informational deficiency. Assessment fatigue arises when governance structures inhibit learning, accountability, and corrective action. By redesigning governance to prioritize action over reporting, critical infrastructure organizations can transform assessment from a symbolic exercise into a meaningful driver of risk reduction and resilience.

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, the integration of the literature, and the preparation of the manuscript.

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.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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 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

Vol. 11, No. 02; 2026

ISSN: 2456-3676

publication. The views expressed in this manuscript are those of the authors and do not necessarily represent the official positions of affiliated organizations.

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

Cybersecurity and Infrastructure Security Agency. (2024). *Cyber Security Evaluation Tool (CSET®)*. https://www.cisa.gov/cset

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://www.nist.gov/cyberframework

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.

Stine, K., Quinn, S., Witte, G., Gardner, R., & Lorenzen, D. (2020). *Integrating cybersecurity and enterprise risk management (ERM)* (NISTIR 8286). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8286