International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Transferability of Cybersecurity Assessment Models 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.2026.11211 URL: http://dx.doi.org/10.51505/ijaemr.2026.11211

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

Abstract

Cybersecurity assessment and maturity models are widely reused across critical infrastructure sectors to evaluate organizational preparedness, demonstrate due diligence, and support governance oversight. This reuse is often premised on an implicit assumption of cross-sector transferability—that assessment constructs, scoring mechanisms, and interpretations retain their meaning regardless of sector context. However, critical infrastructure sectors differ substantially in their missions, governance structures, regulatory environments, and prioritization of consequences. This qualitative, comparative analysis examines the transferability of cybersecurity assessment models across healthcare and energy infrastructure contexts. The study distinguishes assessment elements that remain stable across sectors from those that require contextual or governance adaptation to remain meaningful. It further identifies risks associated with uncritical cross-sector reuse, including false equivalence, governance blind spots, and misaligned decision-making. The article contributes a governance-aware perspective on responsible standardization and provides conceptual guidance for adapting cybersecurity assessment models across diverse critical infrastructure environments.

Keywords: Cybersecurity assessment; transferability; critical infrastructure; governance adaptation; healthcare; energy; maturity models; risk context

1. Introduction

Cybersecurity assessment and maturity models have become foundational tools for evaluating cyber preparedness across critical infrastructure sectors. Frameworks and assessment instruments are routinely applied in healthcare, energy, transportation, and other sectors to benchmark capability, guide investment, and inform governance oversight (Cybersecurity and Infrastructure Security Agency [CISA], 2024; National Institute of Standards and Technology [NIST], 2024).

The widespread reuse of these models reflects an assumption that cybersecurity capabilities can be assessed using standardized constructs that are largely sector-agnostic. Standardization offers

Vol. 11, No. 02; 2026

ISSN: 2456-3676

clear benefits, including comparability, efficiency, and shared language. However, it also raises a critical and under-examined question: to what extent do cybersecurity assessment models retain their meaning when applied across sectors with fundamentally different missions, governance structures, and risk profiles?

Healthcare and energy infrastructure illustrate this challenge. Both sectors rely on complex digital systems and face persistent cyber threats, yet they differ markedly in regulatory drivers, operational coupling, tolerance for disruption, and accountability mechanisms. Applying the same assessment model across these contexts without adaptation risks producing misleading conclusions and governance blind spots.

This article examines the **cross-sector applicability** of cybersecurity assessment models across critical infrastructure sectors. It argues that while certain assessment elements remain stable, others require contextual and governance adaptation to avoid false equivalence and misinformed decision-making. Across this analysis, cybersecurity assessment outputs are treated as interpretive instruments whose meaning and utility depend on governance context, sectoral characteristics, decision authority, and accountability structures, rather than as **fully** self-interpreting or inherently objective indicators of risk.

This manuscript is part of a comprehensive research initiative that examines the interpretation of governance in relation to cybersecurity assessment outcomes in critical infrastructure settings. The series examines the impact of cybersecurity evaluations, maturity models, and governance frameworks on organizational learning, risk assessment prioritization, and resilience in intricate socio-technical systems. By integrating multidisciplinary scholarly analysis with insights from practitioners, the research aims to elucidate how governance design, regulatory environments, and organizational accountability influence the efficacy of cybersecurity risk management and operational resilience.

This study contributes to cybersecurity governance literature by distinguishing between assessment constructs that remain transferable across sectors and those that require governance and contextual adaptation. While prior scholarship has emphasized assessment fidelity and framework design, this analysis highlights the interpretive dimension of assessment outputs and the risks associated with uncritical cross-sector reuse. The study, therefore, advances a governance-aware perspective on the responsible standardization of cybersecurity assessment in critical infrastructure environments.

1.1 Methodological Orientation

This article employs a qualitative, governance-analytic approach grounded in a comparative interpretation of cybersecurity assessment practices across critical infrastructure sectors. Rather than evaluating the technical sufficiency of assessment instruments, the analysis examines the governance architectures through which assessment outputs are translated—or fail to translate—into corrective action. Drawing on governance effectiveness theory, symbolic compliance

Vol. 11, No. 02; 2026

ISSN: 2456-3676

scholarship, and organizational learning frameworks, the study conceptualizes assessment fatigue as a systemic governance outcome rather than as an operational anomaly. The intent is explanatory and conceptual rather than empirical generalization.

2. Background and Context

2.1 Standardized cybersecurity assessment models

In this article, the term cybersecurity assessment outputs refers to the structured findings generated by standardized cybersecurity assessment instruments. Cybersecurity assessment and maturity models are designed to provide a structured evaluation of organizational capabilities. Common features include domain-based scoring, control implementation checks, and maturity progression logic. These models are often promoted as broadly applicable across industries to support consistent risk evaluation and governance reporting (Boyens et al., 2022; NIST, 2024).

2.2 Cross-sector adoption practices

In practice, cybersecurity assessment models are frequently adopted across sectors with minimal modification. Organizations often prioritize efficiency, regulatory alignment, or peer comparability when selecting assessment tools. While this approach streamlines adoption, it assumes equivalence across sector contexts that may not exist.

2.3 Governance and contextual differences between sectors

Critical infrastructure sectors differ in their governance structures, regulatory oversight, and prioritization of consequences. Healthcare organizations operate under patient safety, privacy, and continuity imperatives, while energy systems emphasize grid stability, physical-cyber coupling, and national security considerations (U.S. Department of Energy [DOE], 2022).

These differences shape how cybersecurity risk is interpreted, escalated, and governed. As a result, identical assessment scores may imply materially different risk conditions across sectors.

2.4 Gap in existing analysis

Despite extensive cross-sector use of cybersecurity assessment models, there is limited scholarship that critically examines their boundaries of transferability. Existing literature often emphasizes tool fidelity rather than governance context, leaving a gap in understanding of how the meaning of assessment shifts across sectors. 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

3. Problem Statement

It is not known which elements of cybersecurity assessment models are transferable across critical infrastructure sectors without adaptation to governance.

Uncritical reuse of assessment models risks producing false equivalence, obscuring sector-specific vulnerabilities, and undermining governance decision-making.

4. Purpose of the Study

The purpose of this qualitative comparative analysis is to examine the transferability of cybersecurity assessment models across healthcare and energy infrastructure contexts.

The study focuses on governance interpretation and application of assessment outputs rather than on technical redesign of assessment instruments.

5. Research Questions

RQ1: Which cybersecurity assessment elements remain stable across critical infrastructure sectors?

RQ2: Which assessment elements require contextual or governance adaptation to remain meaningful?

RQ3: What risks arise from uncritical cross-sector reuse of cybersecurity assessment models?

6. Theoretical and Conceptual Framework

This analysis integrates three conceptual perspectives.

Institutional and contextual theory emphasizes how sector norms, missions, and regulatory environments shape organizational meaning. Assessment constructs are interpreted through institutional lenses rather than in isolation.

Governance adaptation theory focuses on how oversight structures, accountability mechanisms, and decision-making authority shape the interpretation and use of assessment outputs.

Risk standardization versus customization theory addresses the tension between comparability and contextual fidelity. While standardization supports benchmarking, customization is often required to preserve risk relevance.

Together, these perspectives support a framework in which assessment transferability depends less on tool design and more on alignment with governance.

Vol. 11, No. 02; 2026

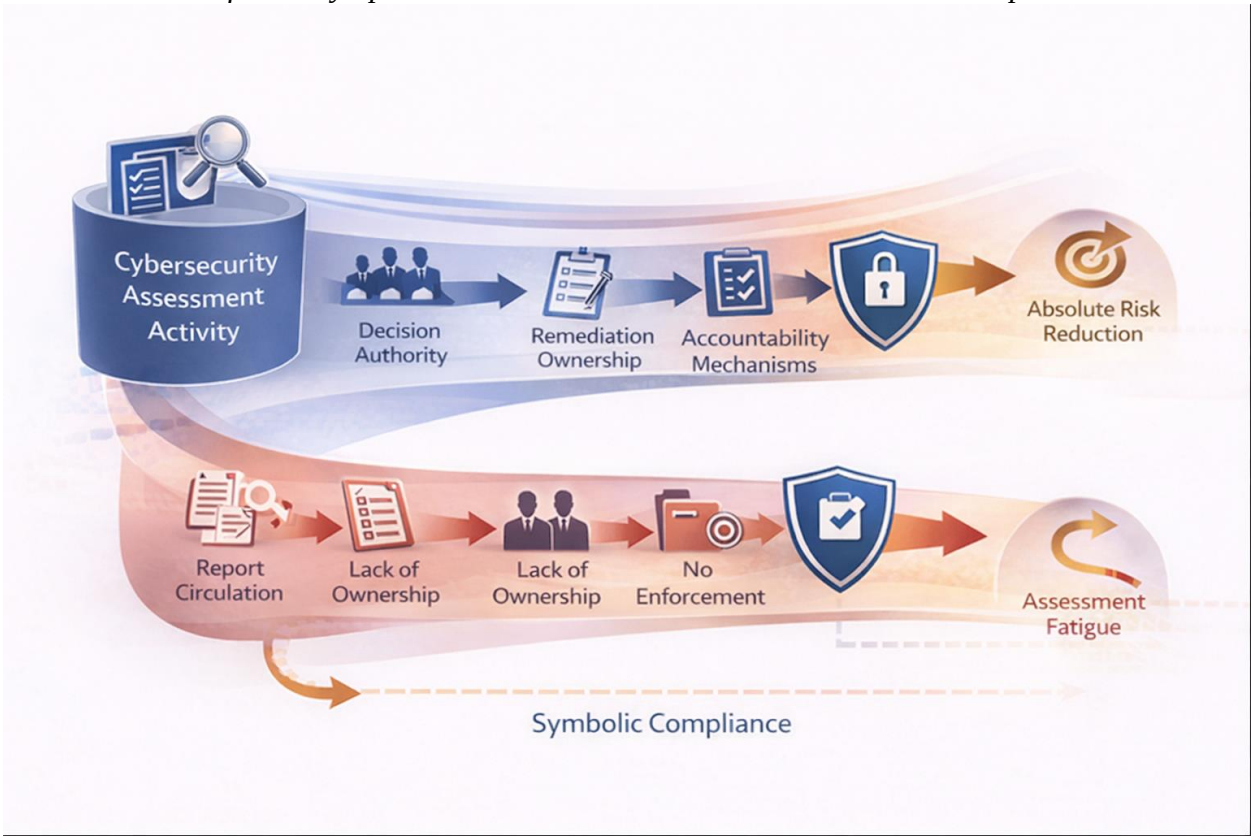
ISSN: 2456-3676

Figure 1 illustrates the governance pathways that follow cybersecurity assessment activity, distinguishing between outcomes driven by accountable remediation and those resulting in symbolic compliance and assessment fatigue.

As conceptualized, cybersecurity assessment activity produces divergent governance outcomes depending on whether findings are translated into accountable remediation or allowed to circulate as symbolic artifacts.

Figure 1

Assessment Transferability Spectrum: Standardization Versus Governance Adaptation



Note. Author created. The figure illustrates two governance pathways following the cybersecurity assessment activity. In the first pathway, findings are linked to decision authority, remediation ownership, and accountability mechanisms, producing measurable risk reduction. In the second pathway, findings circulate through reporting cycles without enforcement or ownership, resulting in symbolic compliance and assessment fatigue. The model is conceptual and intended to illustrate governance dynamics rather than empirical magnitude.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Taken together, these governance pathways reinforce that the effectiveness of cybersecurity assessment is contingent on the translation of findings into accountable action, rather than on the assessment activity itself.

The model underscores that assessment fatigue is not a function of assessment frequency, but of governance architectures that fail to convert evaluation into enforceable action. The model also highlights that cybersecurity assessment constructs fall along a spectrum of transferability. Foundational technical controls often retain meaning across sectors, whereas risk interpretation, impact assessment, and governance prioritization require contextual adaptation.

7. Comparative Analysis of Transferability

Certain cybersecurity assessment elements exhibit high **sectoral generalizability**. These include foundational control domains such as asset management, access control, incident response structure, and basic governance documentation. These elements reflect broadly shared cybersecurity principles and can be meaningfully compared across sectors.

In contrast, other elements require significant contextual adaptation. Impact assessment, recovery prioritization, and acceptable risk thresholds are deeply sector-specific. In healthcare, cyber incidents directly affect patient safety and clinical continuity. In energy systems, cyber disruptions can propagate across interconnected infrastructure with national-level consequences. Unadapted reuse of assessment models risks masking these differences. Identical maturity scores may conceal divergent risk realities, leading governance bodies to draw inaccurate conclusions about preparedness and resilience.

In practice, transferability challenges frequently emerge when organizations adopt assessment models originally developed for different sector priorities. For example, a maturity model emphasizing data confidentiality may translate effectively to healthcare environments where patient privacy is central, yet provide limited insight into operational resilience concerns within energy infrastructure, where physical-cyber coupling and system availability dominate risk priorities. Conversely, models designed for industrial control system environments may overemphasize operational continuity while underrepresenting privacy and compliance considerations critical to healthcare governance. These examples illustrate how sector context shapes both the interpretation of assessment outputs and their governance relevance across different critical infrastructure environments.

Table 1 summarizes the transferability of key cybersecurity assessment elements across critical infrastructure sectors, highlighting which constructs retain meaning and which require governance and contextual adaptation.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Table 1

Transferability of Cybersecurity Assessment Elements Across Sectors

Assessment Element	Transferability	Governance Interpretation
Asset management	High	Foundational cybersecurity control applicable across sectors
Access control	High	Core protection mechanism for both operational and data environments
Incident response structure	Moderate	Generalizable but requires sector-specific escalation logic
Risk impact assessment	Low	Must reflect sector consequences (patient safety vs grid stability)
Recovery prioritization	Low	The sector mission determines acceptable disruption thresholds

Note. Author created. The table summarizes the analytical conclusions, linking the research questions to findings on the cross-sector transferability of cybersecurity assessment constructs. As shown in Table 1, while foundational cybersecurity controls demonstrate high transferability across sectors, governance interpretation of risk, impact, and recovery priorities must be adapted to sector-specific operational realities and accountability structures.

Collectively, these findings demonstrate that cybersecurity assessment transferability is constrained not by the design of the assessment models themselves, but by the governance context in which their outputs are interpreted and applied.

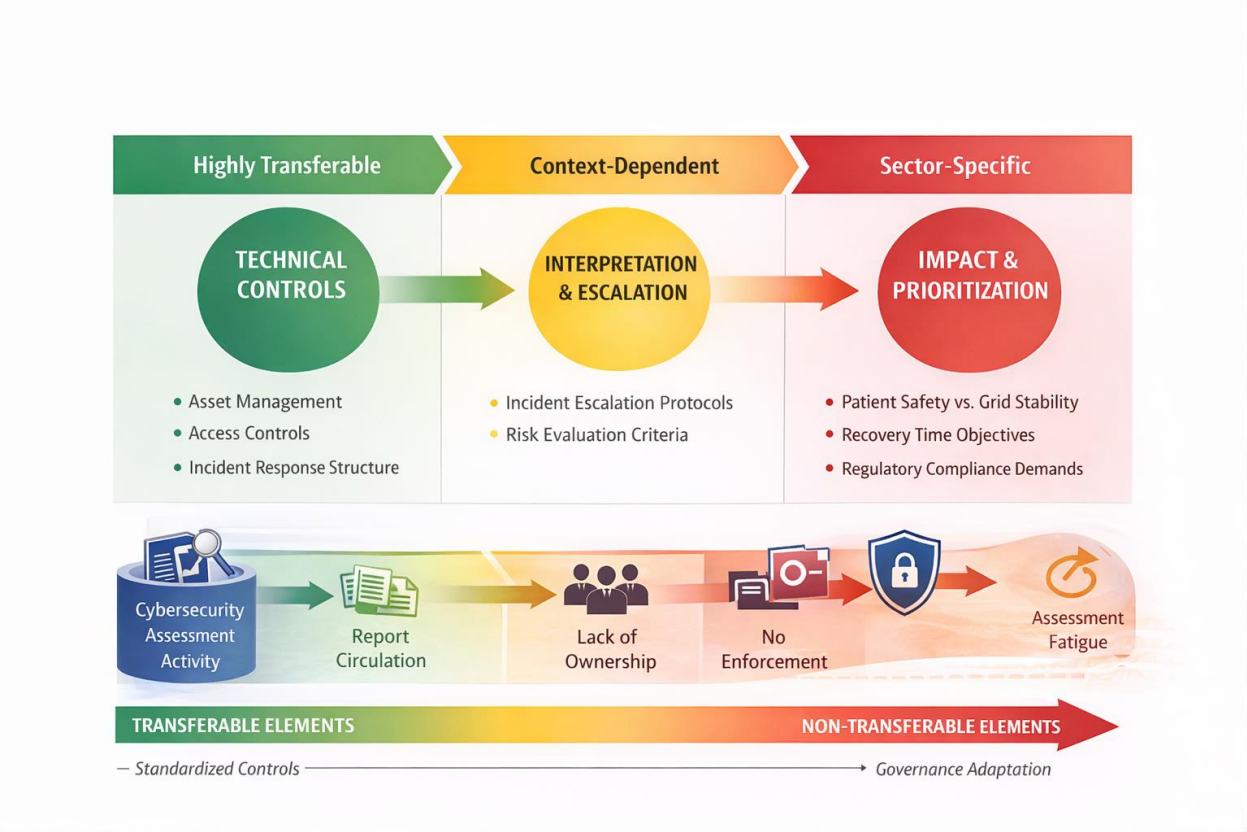
Figure 2 presents a conceptual transferability spectrum that illustrates how cybersecurity assessment elements range from highly transferable technical controls to sector-specific governance interpretations that require contextual adaptation.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Figure 2

Transferability Spectrum of Cybersecurity Assessment Elements



Note. Author created. The figure illustrates the conceptual transferability spectrum of cybersecurity assessment elements, highlighting the progression from highly transferable technical controls to context-dependent interpretation and sector-specific governance adaptation across critical infrastructure environments.

This spectrum underscores that effective cross-sector application of cybersecurity assessments depends on governance-aware adaptation that aligns standardized evaluation outputs with sector-specific risk interpretation and decision-making requirements.

8. Significance of the Study

This study contributes a governance-aware perspective on cybersecurity assessment standardization. It identifies the limits of transferability and clarifies the conditions under which cross-sector reuse is appropriate.

For practitioners, the analysis informs responsible adoption and adaptation of assessment models. For governance bodies, it highlights the importance of contextual interpretation. For

Vol. 11, No. 02; 2026

ISSN: 2456-3676

policymakers and framework designers, it supports the development of assessment guidance that balances comparability with sector relevance.

9. Organization of the Article

The article reviews standardized assessment practices, examines governance and contextual differences between healthcare and energy sectors, identifies transferable and non-transferable assessment elements, and discusses implications for governance and cross-sector adoption.

10. Implications for Governance and Practice

Governance bodies should treat cybersecurity assessment outputs as context-dependent signals rather than absolute indicators. **Cross-domain reuse** should include explicit review of governance assumptions, consequence models, and decision authority.

Implementing governance-aware assessment adaptation can present practical challenges. Organizations may encounter resistance due to institutional inertia, regulatory reporting structures that favor standardized scoring, or limited familiarity with governance in sector-specific risk interpretation. Additionally, cross-sector benchmarking practices may incentivize superficial comparability rather than contextual accuracy. Addressing these barriers requires governance education, explicit adaptation guidance within assessment frameworks, and stronger alignment between sector regulators and cybersecurity oversight expectations.

Assessment models should be adapted through governance overlays rather than technical modification alone. This approach preserves the benefits of standardization while reducing the risk of misinterpretation and false assurance.

Accordingly, responsible standardization requires governance-aware adaptation rather than uncritical model portability across sectors.

11. Limitations and Future Research

This study advances a conceptual governance interpretation of assessment fatigue and does not present empirical measurement of assessment-to-remediation pathways. The analysis does not quantify reductions in incident frequency attributable to governance redesign, nor does it examine longitudinal assessment datasets across multiple organizations. Sectoral illustrations are interpretive and intended to clarify governance dynamics rather than to generalize prevalence across critical infrastructure domains. Future research may examine assessment fatigue through structured governance audits, comparative case studies, and empirical evaluation of remediation-tracking mechanisms to determine how accountability structures influence measurable reductions in cyber risk.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

12. Conclusion

Cybersecurity assessment models offer valuable structure and comparability, but their meaning is not inherently transferable across critical infrastructure sectors. Transferability depends on the governance context, sector mission, and prioritization of consequences. Uncritical reuse risks obscuring material differences and weakening oversight. A governance-aware approach to assessment transferability supports more accurate interpretation, stronger decision-making, and more resilient critical infrastructure systems. Even when assessment models are appropriately adapted across sectors, repeated assessment can still fail to reduce risk if governance structures do not translate outputs into accountable action—a failure mode examined in subsequent analyses of assessment fatigue and governance design.

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.

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

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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

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

U.S. Department of Energy. (2022). *Cybersecurity Capability Maturity Model (C2M2), Version 2.1*. https://www.energy.gov

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

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.