International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

From Compliance to Resilience: Reframing Cybersecurity Maturity Models for Executive Decision-making in Critical Infrastructure

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

doi.org/10.51505/ijaemr.2026.1203 URL: http://dx.doi.org/10.51505/ijaemr.2026.1203

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

Abstract

Cybersecurity maturity models are widely used across critical infrastructure sectors to assess security posture and demonstrate alignment with regulatory and industry expectations. However, maturity results are frequently interpreted as compliance achievements rather than as resilience-relevant decision inputs for executives, boards, and policymakers. This article argues that cybersecurity maturity models realize their greatest value when reframed as executive decision-support mechanisms that link cybersecurity capabilities to enterprise risk, operational resilience, and supply chain interdependence. Drawing on critical-infrastructure contexts in healthcare supply chains and energy and smart-grid governance, the article proposes a resilience-oriented interpretive framework that transforms maturity outputs into governance-grade insights, including capability distribution, weakest-link exposure, prioritized investment logic, and continuous improvement pathways. The resulting contribution offers a practical and defensible approach for translating maturity assessments into board-level oversight, strategic planning, and risk-informed resource allocation in complex, interdependent infrastructure ecosystems.

Keywords: cybersecurity maturity models; executive decision-making; governance; resilience; critical infrastructure; enterprise risk management; C2M2; NIST CSF 2.0

1. Introduction

Across critical infrastructure sectors, cybersecurity maturity models have become standard instruments for evaluating cybersecurity capability, benchmarking performance, and demonstrating due diligence. Maturity-based approaches are often preferred to checklist-style audits because they characterize cybersecurity as a staged capability that can be institutionalized and strengthened over time. Despite these advantages, maturity outcomes are frequently treated as compliance indicators or scorekeeping mechanisms rather than as decision inputs that inform resilience, enterprise risk management, and strategic governance (Shawe, 2026).

This compliance-centric framing creates a governance gap. Executives and boards are accountable for risk acceptance, prioritization, and oversight. However, they often receive maturity results as static levels or aggregate scores that fail to communicate operational

Vol. 11, No. 02; 2026

ISSN: 2456-3676

implications, systemic exposure, or investment urgency. In interdependent environments—where supply chain partners and internal organizational units exhibit uneven cybersecurity capability—simplified maturity reporting can obscure the very conditions that drive systemic cyber risk (Mengnjo, 2026; Shawe, 2026).

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. This article argues that cybersecurity maturity models must be reframed from compliance-reporting tools into resilience-oriented decision-support systems. Building on doctoral research in healthcare supply chain cybersecurity assessment and energy and smart-grid governance, and aligned with widely used public-sector frameworks and assessment tools, the study proposes an executive interpretation approach that translates maturity results into actionable governance insights (National Institute of Standards and Technology [NIST], 2024; U.S. Department of Energy [DOE], 2022; Cybersecurity and Infrastructure Security Agency [CISA], 2024).

This manuscript constitutes a segment of an extensive research initiative that explores the governance perspectives on cybersecurity assessment outcomes within critical infrastructure settings. The series scrutinizes the influence of cybersecurity assessments, maturity models, and governance frameworks on organizational learning, risk management priorities, and resilience in complex socio-technical systems. By integrating multidisciplinary academic analysis with practitioner-informed insights, the research aims to elucidate how governance frameworks, regulatory environments, and organizational accountability impact the efficacy of cybersecurity risk management and operational resilience.

1.1 Methodological Orientation

This article employs a qualitative conceptual analysis grounded in governance theory, resilience theory, and scholarship on executive decision-making. The approach synthesizes established cybersecurity maturity models—including C2M2 and CSF 2.0—with risk governance and resilience frameworks to examine how maturity outputs are interpreted at executive and board levels.

The analysis does not attempt to quantify the effectiveness of maturity or conduct empirical validation. Instead, it develops an interpretive framework that distinguishes compliance-oriented reporting from resilience-oriented governance application. Healthcare and energy infrastructure contexts are used illustratively to demonstrate how maturity outputs can be reframed as decision-support mechanisms.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

2. Background and Context

2.1 Why Maturity Models Became Central in Critical Infrastructure

Cybersecurity maturity models are widely adopted because they provide an interpretable representation of cybersecurity capability—not merely whether controls exist, but whether practices are repeatable, institutionalized, and improving. In critical infrastructure environments, where information technology (IT) systems intersect with operational technology (OT) systems that monitor and control physical processes, maturity models support phased improvement planning, roadmap development, and executive communication (DOE, 2022; Shawe, 2026).

The Cybersecurity Capability Maturity Model (C2M2) provides a structured, maturity-based framework for improving preparedness and response capabilities across organizational units and operational environments (DOE, 2022). Similarly, the NIST Cybersecurity Framework (CSF) 2.0 provides an outcomes-oriented structure that supports governance, resilience, and risk communication across organizational functions and interdependent partners (NIST, 2024). These frameworks are commonly used in critical infrastructure governance contexts because they provide shared language across technical, managerial, and executive audiences.

2.2 The Compliance Trap: Maturity as a Score Rather Than a Decision Input

Despite their design intent, maturity models are often implemented as compliance mechanisms. Maturity levels become targets in themselves, and reporting focuses on achievement rather than operational consequence. This dynamic is particularly problematic in supply chain ecosystems, where cybersecurity capability is unevenly distributed across vendors and internal units. Evidence from healthcare supply chain assessments demonstrates that weakest-link exposure can dominate system-level risk regardless of average or enterprise-level maturity (Mengnjo, 2026; Boyens et al., 2022).

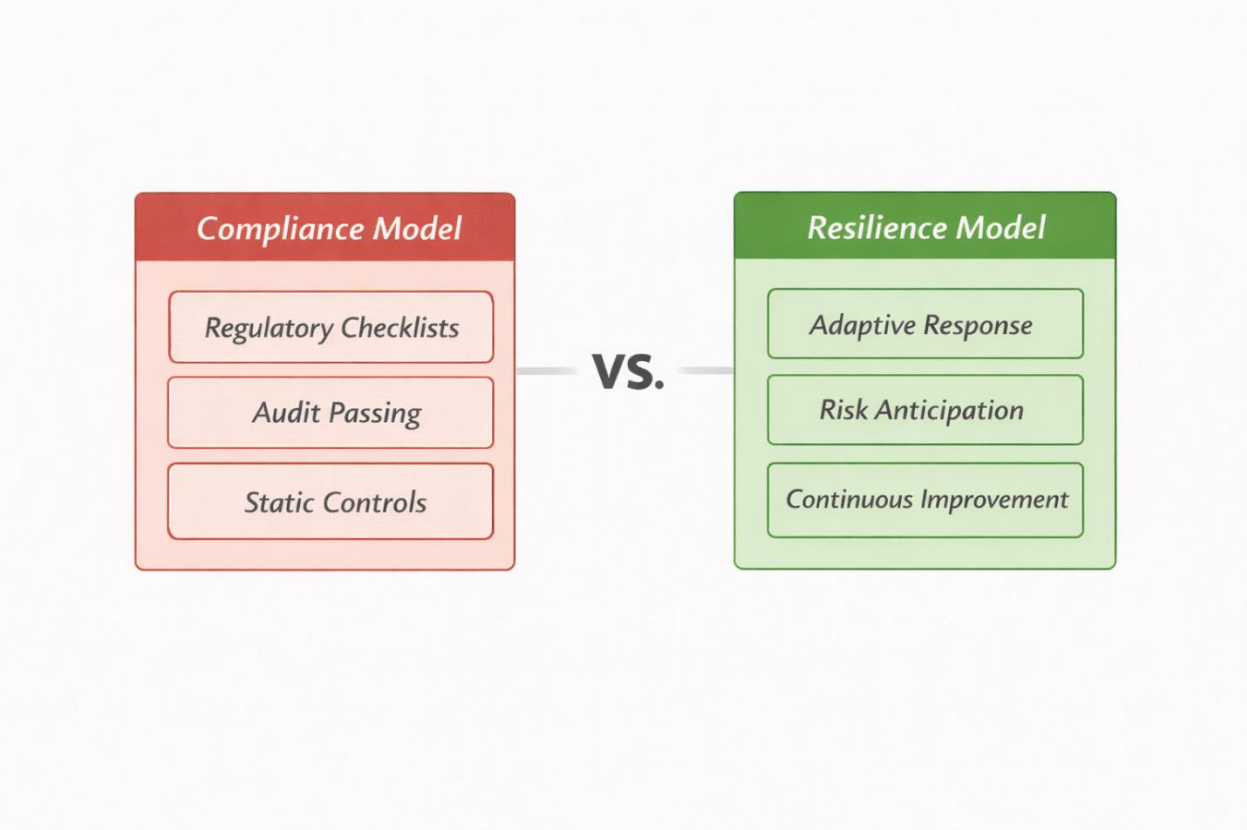
In energy and smart-grid environments, governance similarly requires that maturity outputs be interpreted to support risk-informed decision-making and resilience planning rather than static compliance snapshots (Shawe, 2026). When maturity is reduced to a score, leadership loses visibility into variation, trends, and interdependence—precisely the dimensions that determine resilience in complex infrastructure systems. 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). To illustrate the interpretive distinction between compliance-oriented maturity reporting and resilience-oriented governance interpretation, the conceptual comparison presented 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 summarizes two interpretive frames for the outputs of a cybersecurity maturity model. The compliance-oriented frame emphasizes attainment and audit satisfaction, whereas the resilience-oriented frame emphasizes adaptive capacity, risk anticipation, and continuous improvement as governance-relevant inputs for decision-making. The model is conceptual and supports the interpretive framework developed in this article.

The conceptual distinction between compliance-oriented maturity interpretation and resilience-oriented maturity interpretation is illustrated in Figure 1.

3. Problem Statement

Although cybersecurity maturity models are widely used across critical infrastructure sectors, there is no consistent approach to interpreting maturity outputs to support executive decision-making on resilience and the reduction of systemic risk. Current practices often frame maturity results as compliance achievements or summary scores, obscuring the distribution of capabilities, the weakest-link exposure, and the operational implications of interdependence across supply chains and internal organizational units (Mengnjo, 2026; Shawe, 2026).

Vol. 11, No. 02; 2026

ISSN: 2456-3676

4. Purpose of the Study

The purpose of this qualitative, governance-focused analysis is to develop a resilience-oriented approach for interpreting cybersecurity maturity model outputs as executive decision support. By integrating healthcare supply chain assessment evidence with energy and smart-grid governance insights, and aligning interpretations with NIST-aligned risk management and improvement structures, the study proposes a practical framework that translates maturity findings into prioritized actions, oversight narratives, and continuous improvement pathways (NIST, 2024; DOE, 2022; Mengnjo, 2026; Shawe, 2026).

5. Research Questions

1. How are cybersecurity maturity model results commonly interpreted and reported to executives and boards in critical infrastructure sectors?
2. What resilience-relevant insights are lost when maturity outputs are treated primarily as compliance scores?
3. How can maturity outputs be reframed to support governance, prioritization, and systemic resilience planning across interdependent infrastructures?

6. Conceptual and Theoretical Framework

This study integrates three complementary perspectives:

Risk governance and executive oversight. Effective governance depends on actionable, comparable information that connects cybersecurity capability to risk acceptance and resource allocation (NIST, 2024; Shawe, 2026).

Resilience framing. Resilience extends beyond the presence of controls to include the ability to anticipate, withstand, respond to, and recover from disruption, particularly in interdependent environments (Shawe, 2026).

Supply chain risk logic. Systemic exposure is shaped by weakest-link dynamics and interorganizational dependencies, requiring visibility into capability distribution rather than enterprise averages (Mengnjo, 2026; Boyens et al., 2022).

Within this framework, cybersecurity maturity models are treated as decision artifacts rather than compliance artifacts. Maturity outputs become governance-relevant when they answer executive questions such as: Where is capability weakest? Which weaknesses drive systemic exposure? What investments most effectively reduce risk? How is improvement tracked over time?

7. Reframing Maturity Outputs for Resilience-Oriented Executive Decision-Making

This section proposes a practical reframing approach that transforms maturity results into governance-grade insights. The approach can be applied using maturity models such as C2M2 and structured assessment instruments such as the Cyber Security Evaluation Tool (CSET®),

Vol. 11, No. 02; 2026

ISSN: 2456-3676

with findings expressed using CSF-aligned outcomes language (CISA, 2024; DOE, 2022; NIST, 2024).

7.1 From Maturity Level to Capability Distribution

Executive reporting should emphasize the distribution of capabilities across organizational units and partners rather than aggregate maturity levels. Healthcare supply chain assessments show that uneven capability across vendors and internal units can dominate systemic risk even when enterprise reporting appears satisfactory (Mengnjo, 2026). Energy and smart-grid governance similarly requires visibility into uneven implementation across interconnected system components (Shawe, 2026).

7.2 Translating Maturity Gaps into Operational Consequences

Maturity gaps must be interpreted in terms of operational outcomes such as service continuity, safety, regulatory exposure, and recovery capability. In healthcare environments, gaps in third-party risk management and incident response coordination can cascade across care delivery operations (Mengnjo, 2026). In energy systems, governance-aligned capability gaps can propagate systemic vulnerabilities across interconnected infrastructure (Shawe, 2026).

7.3 Prioritizing Investment Using Weakest-Link Logic

A resilience-oriented interpretation prioritizes investments that reduce systemic exposure by strengthening the most vulnerable capability concentrations. Supply chain risk management guidance emphasizes integrating dependency risk into organizational risk management processes and systematically addressing exposure concentrations (Boyens et al., 2022).

7.4 Using Structured Assessments as Governance Evidence

Structured assessment mechanisms such as CSET support repeatable, evidence-based evaluation. When paired with a resilience-oriented interpretation, assessment outputs can be communicated as governance evidence rather than as technical detail, thereby supporting executive oversight and accountability (CISA, 2024; Mengnjo, 2026; Shawe, 2026).

7.5 Treating Maturity as a Trendline

Resilience planning requires longitudinal insight. Governance should track maturity progression over time and across domains rather than relying on point-in-time snapshots. This approach aligns with the principles of continuous improvement and continuous monitoring embedded in risk management frameworks (Joint Task Force, 2018; DOE, 2022).

Vol. 11, No. 02; 2026

ISSN: 2456-3676

8. Sector Illustrations

8.1 Healthcare Supply Chains

Healthcare supply chains illustrate the risks of interpreting compliance-centric maturity. Enterprise-level reporting often obscures vendor and unit-level variability, reducing visibility into weakest-link exposure. Assessment-based research demonstrates that differences in cybersecurity capability across partners shape systemic risk and operational vulnerability (Mengnjo, 2026).

8.2 Energy and Smart-Grid Infrastructure

Energy and smart-grid environments require governance models that align cybersecurity capability with reliability and resilience outcomes. When maturity outputs are reframed as decision inputs rather than compliance scores, executives can better align cybersecurity investments with operational resilience objectives (DOE, 2022; NIST, 2024; Shawe, 2026).

9. Governance Implications and Practical Recommendations

This analysis yields five governance recommendations:

1. Require capability distribution reporting across units and vendors.
2. Link maturity findings to operational and mission consequences.
3. Prioritize weakest-link remediation to reduce systemic exposure.
4. Pair maturity reporting with structured assessment evidence.
5. Track maturity as a longitudinal trend rather than a snapshot.

10. Contribution and Significance

This article contributes to cybersecurity governance and resilience literature by reframing maturity models as executive decision-support mechanisms. Rather than treating maturity as a compliance target, the study positions maturity outputs as governance-grade inputs that surface **disproportionate risk drivers** and inform resilience-oriented investment and oversight (Mengnjo, 2026; Shawe, 2026).

11. Conclusion

Cybersecurity maturity models are essential tools in critical infrastructure environments, but their governance value is diminished when interpreted solely through a compliance lens. In interdependent systems, resilience depends on the distributional visibility and **outlier-driven risk identification**. By reframing maturity outputs as executive decision support—grounded in structured assessment evidence, weakest-link prioritization, and trend-based improvement—organizations can strengthen oversight, allocate resources more effectively, and reduce systemic cyber risk across critical infrastructure ecosystems.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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 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.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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

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

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 Cybersecurity 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://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.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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