International Journal of Advanced Engineering and Management Research

Vol. 11, No. 06; 2026

ISSN: 2456-3676

Artificial Intelligence Governance Maturity Model (AIGMM): A Capability-Based Framework for Organizational Assessment, Continuous Improvement, and Trustworthy AI

Dr. Robb Shawe (Lead Author)[1], Dr. Robert W. Clark (Co-Author)[1]
[1]Department of Sustainability and Department of Cyber-Psychology
Capitol Technology University, 11301 Springfield Road, Laurel, Maryland, USA

doi.org/10.51505/ijaemr.2026.11606 URL: http://dx.doi.org/10.51505/ijaemr.2026.11606

Received: Nov 12, 2026 Accepted: Nov 20, 2026 Online Published: Nov 27, 2026

Abstract
Organizations need evidence that artificial intelligence (AI) governance practices are implemented consistently and improved based on operational experience. This conceptual article presents the Artificial Intelligence Governance Maturity Model (AIGMM), which organizes governance capability into eight domains and five cumulative maturity levels. A targeted synthesis links governance, risk management, organizational capability, socio-technical systems, and organizational learning to the model's design. The proposed assessment combines domain-specific evidence with common scoring criteria, independent review, and a conservative rule that sets overall maturity at the lowest supported domain level when all eight domains can be rated. A hypothetical critical infrastructure assessment demonstrates how the rules are applied and how differences between assessors are resolved. AIGMM offers a structured basis for identifying capability gaps and planning reassessment. Its rating reliability, validity, and effects on organizational outcomes remain open empirical questions.

Keywords: artificial intelligence governance, governance maturity model, organizational capability, AI risk management, continuous improvement, trustworthy AI, adaptive governance, organizational assessment

1. Introduction

Organizations increasingly use artificial intelligence (AI) in decisions that affect service delivery, resource allocation, and operational safety. An enterprise can issue an AI policy and still lack evidence that personnel follow it across units, that review occurs when required, or that findings lead to verified changes. Governance maturity concerns how consistently these practices are established, implemented, monitored, and improved.

The first article in this series proposes the Artificial Intelligence Governance Framework for Critical Infrastructure (AIG-CI), which defines governance responsibilities and lifecycle checkpoints (Shawe & Clark, 2026a). The second proposes the Artificial Intelligence Governance Assurance (AIGA) Framework, which specifies how operators can produce

Vol. 11, No. 06; 2026

ISSN: 2456-3676

evidence through decision records, monitoring, exception handling, and verified corrective action (Shawe & Clark, 2026b). AIGMM uses such records to assess the sustained capability of a defined organizational scope. An AIGA record can demonstrate that a control operated in a particular event. AIGMM additionally examines coverage, recurrence, and improvement across events and units.

The guiding question is how an organization can translate varied governance evidence into reproducible maturity judgments across eight capability domains. This study proposes the domain structure, level criteria, and scoring rules and applies them to one hypothetical assessment.

2. Literature Review

2.1 Governance and Organizational Capability

AI governance instruments address leadership, oversight, risk management, and responsible operation. Organizational capability research explains why assessing these responsibilities requires attention to recurring routines, coordinated resources, and the ability to revise them over time (Teece et al., 1997; Winter, 2003). The presence of a written policy supports a finding about formalization. Evidence that personnel use it across units and act on findings supports a different judgment about implementation.

2.2 Maturity Assessment

Maturity-model research distinguishes model design, measurement, testing, and deployment. It supports defining a bounded scope, making successive levels observable, and evaluating the assessment instrument empirically (Becker et al., 2009; de Bruin et al., 2005; Wendler, 2012). AIGMM applies this distinction by treating the proposed rubric and aggregation rule as design choices whose reliability and consequences can be tested.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

2.3 Governance and Maturity Comparators

Table 1 compares AIGMM with the National Institute of Standards and Technology AI Risk Management Framework (NIST AI RMF), ISO/IEC 42001, the MITRE AI Maturity Model, and the U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2). The comparison examines scope, evidence, and output.

Table 1. Comparison of Governance and Maturity Assessment Approaches

Approach	Scope	Evidence or assessment basis	Output
NIST AI RMF 1.0	AI risk management across the lifecycle	Context, risk measurements, controls, and monitoring organized by outcomes and actions	Risk and trustworthiness outcomes and actions for the relevant use case or profile
ISO/IEC 42001:2023	Organizational AI management system	Management-system documentation and evidence that processes and controls operate	Requirements against which system conformity can be evaluated
MITRE AI Maturity Model and Assessment Tool	Enterprise AI adoption, including responsible use and governance	Evidence prompts and level descriptions across 20 dimensions in six pillars	AI maturity assessment across adoption dimensions
DOE C2M2 v2.1	Cybersecurity capability in an organization or function	Implementation ratings for practices organized by domain and maturity indicator level	Achieved maturity indicator levels by cybersecurity domain
AIGMM (proposed)	Institutionalization of AI governance within a defined organizational scope	Domain-specific evidence evaluated against five cumulative levels and adjudicated if needed.	Eight domain ratings and, when all are rateable, an overall level based on the lowest domain

Note. Sources are Tabassi (2023), ISO/IEC (2023), MITRE (2023), and the U.S. Department of Energy (2022). The comparison concerns design and scope. Conformity, score equivalence, and comparative effectiveness are outside its scope.

MITRE already assesses governance and responsible use within broader enterprise AI adoption. C2M2 already uses cumulative domain-level progression in cybersecurity. AIGMM's proposed contribution is combining eight governance-specific domains, common evidence requirements across those domains, and a conservative overall level that makes the least-developed capability visible. The comparison does not establish that this combination yields more accurate judgments or better organizational outcomes.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

3. Theoretical Foundations of the Artificial Intelligence Governance Maturity Model

Governance theory and AI management guidance inform the separation of executive accountability, policy, and external accountability (Bevir, 2013; ISO/IEC, 2023). Enterprise risk management informs the risk ownership and treatment domain (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017). Organizational capability theory supports asking whether practices recur across units and survive changes in personnel or technology (Teece et al., 1997; Winter, 2003).

Socio-technical systems theory informs the distinction among technical assurance, the operational use of controls, and the competence of the people responsible for them (Trist & Bamforth, 1951; Walker et al., 2008). Organizational learning and adaptive governance inform the separate requirement to act on findings, verify changes, and revise routines after material changes in context (Argyris & Schön, 1978; Folke et al., 2005). These theoretical links explain the design choices. They do not establish that the domains are statistically distinct or causally related to performance.

4. Model Development Methodology

4.1 Research Design and Source Selection

AIGMM was developed through conceptual model construction supported by a targeted narrative synthesis and comparison. The source set centers on published material directly relevant to at least one design question: which AI governance responsibilities belong within the enterprise scope, how those responsibilities become institutionalized, or what evidence indicates progression. The governance sources include NIST AI RMF and ISO/IEC 42001. Maturity-model scholarship and the Capability Maturity Model for Software inform stage design. MITRE and C2M2 provide comparison cases for the revised model. The comparison is selective and does not estimate the prevalence or effectiveness of competing approaches.

4.2 Analytical Procedure and Domain Derivation

Three design steps explain the domain derivation. First, identify the governance responsibility or maturity characteristic each source addresses. ISO/IEC 42001 and the NIST AI RMF informed the separation of leadership, policy, lifecycle assurance, and stakeholder accountability (ISO/IEC, 2023; Tabassi, 2023). COSO informed the enterprise risk domain (COSO, 2017). Socio-technical systems and organizational learning scholarship informed operational integration, workforce competency, and continuous improvement (Argyris & Schön, 1978; Trist & Bamforth, 1951; Walker et al., 2008). Second, group overlapping responsibilities by who performs the practice and which evidence demonstrates it. For example, executive authorization maps to strategic leadership, whereas routine checks that an authorized workflow was used map to operational integration. Third, check that each domain has a distinct assessable responsibility, a theoretical basis, and examples of observable evidence. Table 2 shows the resulting mapping. The same record may support separate criteria.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

4.3 Maturity Level Derivation

The Capability Maturity Model for Software and maturity-model development literature inform the use of ordered stages (Becker et al., 2009; de Bruin et al., 2005; Paulk et al., 1993). The AIGMM stages distinguish five observable conditions: localized or reactive practice, emerging documented adoption, standardized implementation across scope, repeated monitoring with verified response, and adaptation followed by review of the change. These distinctions explain why a policy alone does not meet Defined and why a dashboard alone does not meet Managed. Section 6 converts the stages into proposed cumulative rating criteria.

4.4 Conceptual Coherence

Conceptual coherence depends on whether the evidence required at each stage matches the corresponding capability and whether higher levels retain the practices required at lower levels. The domain mapping and the worked example make this reasoning visible. The resulting framework awaits testing with independent assessors and organizational records.

5. Artificial Intelligence Governance Maturity Model (AIGMM)

5.1 Framework Overview

AIGMM evaluates eight complementary governance capabilities within a defined assessment scope. A domain can mature at a different rate from other domains. Assessors record the eight ratings separately before deriving an overall level.

Figure 1 shows how the eight governance domains relate to the five maturity levels and how findings inform subsequent assessment.

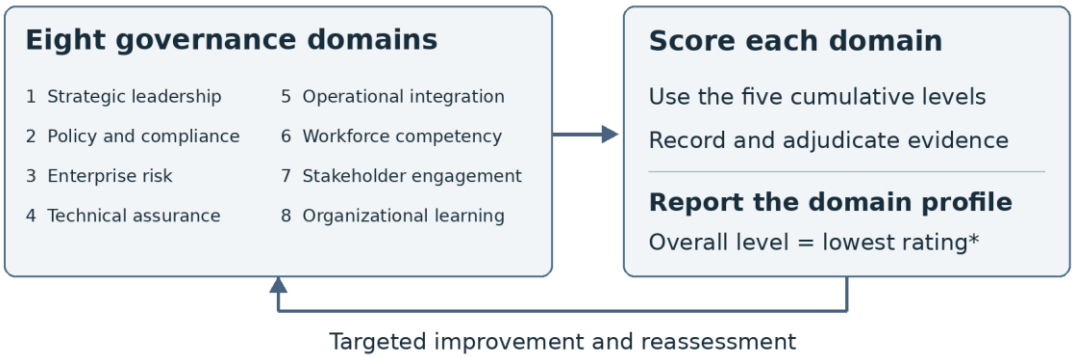


Figure 1. Artificial Intelligence Governance Maturity Model

Note. Authors' conceptual framework. * An overall level is assigned only when all eight domains are rated. The feedback loop represents using assessment findings to guide corrective action and reassessment.

The architecture separates the capability being assessed from the level demonstrated by the evidence. Table 2 defines the responsibilities and observable practices that distinguish the eight capabilities.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

5.2 Governance Capability Domains

Table 2 traces the eight domains to their underlying constructs and gives examples of practices and records an assessor can examine.

Table 2. Domain Derivation and Observable Governance Evidence

Capability domain	Underlying construct	Observable practice	Example evidence
1. Strategic Leadership and Executive Oversight	Executive accountability and direction	Assign decision authority and review risk, resource, and escalation decisions.	Approved charter, delegations, executive minutes, and tracked decisions.
2. Governance Policies and Regulatory Compliance	Normative requirements and policy control	Maintain current rules, map obligations, and review policy exceptions.	Approved policies, obligations register, policy change and exception records.
3. Enterprise Risk Management	Risk ownership, treatment, and monitoring	Evaluate AI risks, assign treatments, and verify action on material risks.	Risk register, treatment approvals, monitoring reviews, and verified actions.
4. Technical Assurance and AI Lifecycle Management	Lifecycle control and technical verification	Validate model versions, review evidence at release, and monitor operation and change.	Local evaluation reports, model registry, release records, and monitoring logs.
5. Operational Integration	Control execution within routine work	Apply required oversight and escalation through operating, procurement, or approval workflows.	Workflow records, approval and override logs, escalation and vendor review records.
6. Workforce Competency and Organizational Culture	Sustained competence and accountability	Define role-based competence and check that staff can perform or challenge covered decisions.	Training and practical assessment records, assignment records, and escalation exercises.
7. Stakeholder Engagement and Transparency	External accountability and contestability	Provide relevant notice, collect feedback, and document responses and escalation.	Notices, feedback or complaint register, and response records.
8. Continuous Improvement and Organizational Learning	Learning from findings and verified change	Assign improvement actions, verify closure, and use findings to revise practice.	Audit findings, action register, closure checks, and follow-up reviews.

Note. The records are examples. Assessors may use equivalent evidence if it demonstrates the same practice. The citations in Section 3 and the source comparison in Table 1 explain the theoretical and comparative basis.

The same release file may contain evidence for more than one domain. A validation report can support technical assurance, while the approval and exception records can support operational integration. Each domain is rated against its own criterion.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

5.3 Maturity Hierarchy

Figure 2 shows how evidence requirements progress from localized practice to verified adaptation.



Figure 2. Five Levels of AI Governance Maturity

Note. Levels are cumulative and ordinal. The sequence represents increasing institutionalization and supplies no assumption of equal distances between levels.

The five levels describe evidence requirements, including the possibility that a scope falls back to a lower level when practices lapse. Section 6 specifies how to apply these requirements and report uncertainty.

6. Organizational Assessment Methodology

6.1 Scope and Evidence Collection

The unit of assessment is a named organization or organizational scope during a defined review period. Before reviewing evidence, document the included units, AI use cases, governance responsibilities, and assessment period. Define applicable practices and expected review cadences. Include all units in the scope and all material-risk use cases. For other use cases or recurring records, specify and record the sampling method and the reason for the sample. Results describe the assessed scope and evidence.

For each domain, retain the applicable criterion, artifacts, dates, responsible owners, units or use cases covered, and any contradictory information in an evidence register. Use contemporaneous operational records for implementation, repeated performance, and verified change. Interviews may clarify the records. Policy text and self-reports alone cannot establish that a practice operated. Record and justify any inapplicable indicator before scoring. Retain all eight domains in the assessment and record a domain as insufficient evidence when a defensible equivalent cannot be assessed.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

6.2 Domain Scoring and Overall Level

Table 3 defines the minimum evidence for each of the five cumulative maturity levels. Apply the criteria to the practices in scope for each domain.

Table 3. Cumulative Rating Criteria for Each Governance Domain

Level	Observable threshold	Minimum evidence
1. Initial (Ad Hoc)	Practice is absent, reactive, or dependent on local initiative.	Scope review documents the absence of an established practice or shows isolated or reactive execution.
2. Developing	A responsible role and at least one documented practice are evident, with at least local or pilot adoption.	A role assignment and a dated local procedure, pilot record, or equivalent evidence of initiation.
3. Defined	An approved practice is in use in every applicable unit and in all material-risk cases and other records assessed under the sampling rule.	Current standard and accountable roles, plus operating records across the defined scope. A material uncovered case prevents Level 3.
4. Managed	The defined practice is reviewed against stated criteria in at least two completed scheduled cycles. Findings are acted on and completed actions are verified.	Dated records of two distinct reviews, measures against targets, and dispositions and verified closure for completed actions. Document reviews that produced no findings.
5. Adaptive (Optimized)	A documented change in risk or a recurring finding prompts an approved adjustment, followed by checks of its effect and uptake in affected units.	Traceable finding or change trigger, approved adjustment, evidence of implementation, and follow-up evaluation against defined expectations.

Note. Two completed review cycles are a proposed minimum for observing repeated management. Cycle length follows the documented cadence for the practice. The criteria and overall aggregation rule require empirical evaluation.

Rate each domain at the highest level whose applicable criteria and lower-level capabilities are supported. An enterprise-wide practice can establish lower-level requirements without historical records of earlier stages when current evidence supports those requirements. A known failure at a higher level limits the rating to the highest lower level demonstrated. If essential evidence is unavailable or contradictory and could change the rating, record insufficient evidence and, where possible, the highest level already demonstrated as a provisional lower bound. Assign Level 1 when reviewed evidence shows localized or reactive practice, or establishes that the relevant practice is absent. Missing records alone do not establish Level 1.

Two assessors should independently review the evidence and record their initial ratings with reasons. When ratings differ, compare the disputed criterion, evidence dates and coverage, and any conflicting records. Both assessors record the resulting rationale. If disagreement persists, a third assessor reviews the evidence and records an adjudicated finding. If the evidence remains

Vol. 11, No. 06; 2026

ISSN: 2456-3676

indeterminate, mark the affected domain insufficient evidence and specify what is needed for resolution.

Report the eight confirmed ratings together. When all eight are rated, the overall level is the minimum of the eight ratings: it is the highest level supported across every domain. Do not average the ordinal scores. When any domain is marked insufficient evidence, withhold the overall level and report the confirmed ratings and any supported lower bounds. A high-rated domain can still inform improvement planning, and a finding with serious consequences warrants action regardless of its effect on the overall level.

6.3 Hypothetical Worked Assessment

Consider a fictional regional electric utility assessing maintenance prioritization and outage triage over six months. The scope covers both business units and all three material-risk AI use cases. The assessors review all three use cases and the applicable records from both units, including scheduled approvals, quarterly reviews, model version records, training records, stakeholder feedback, and corrective actions. The records and ratings below are invented solely to illustrate the procedure.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

Table 4 summarizes the evidence that supports each of the eight ratings and explains why the next level is not assigned.

Table 4. Hypothetical Utility Assessment and Domain Ratings

Domain	Evidence supporting the assigned level	Level	Why the next level is not shown
1. Leadership	Charter and delegations apply across both units. Two quarterly reviews tracked resource decisions and verified completed actions.	4	No adjustment with follow-up evidence of effect.
2. Policy and compliance	Both units use an approved policy and current obligations register, evidenced in the three case files.	3	Only one scheduled policy-control review was completed.
3. Enterprise risk	All case risks have owners. Two reviews tested treatment against criteria and verified completed actions.	4	No evidence of a material risk-driven adjustment and follow-up.
4. Technical assurance	All current versions have local validation and release records. One monitoring review was completed.	3	The second scheduled monitoring review was missed.
5. Operational integration	All three use cases use standard decision approvals and documented escalation routes in both units.	3	No repeated workflow performance review.
6. Workforce competency	Both units have assigned roles and completed role-based training and practical checks.	3	No repeated evaluation of competency results and follow-up.
7. Stakeholder engagement	A feedback owner and documented intake process operate in one unit. The other unit handles feedback informally.	2	A common process is not operating in both units.
8. Organizational learning	Both units use an action register. Two reviews verified closures against the stated criteria.	4	No approved change with a follow-up evaluation of its effects across affected units.

Note. This hypothetical example contains no observed organizational results. The evidence summaries assume the two assessors reviewed the records in the stated scope.

The assessors initially rated Technical Assurance at Levels 4 and 3. The first assessor counted a release authorization as a second monitoring cycle. Reconciliation showed that it was a release decision and that the cutoff did not complete the second scheduled monitoring review. Local validation and release controls were documented and applied throughout the scope, so both assessors assigned Level 3. With the agreed profile of 4, 3, 4, 3, 3, 3, 2, and 4, the overall rating is Level 2 (Developing). Stakeholder Engagement and Transparency limits the overall level. A first improvement is to establish and document a common feedback and response process across both units, then verify that it operates before reassessment.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

6.4 Reporting and Reassessment

Use the profile to identify evidence gaps, compare repeated assessments within the same scope, and prioritize corrective action. Retain the scope, evidence window, and rating criteria across assessments or document changes that affect comparability. Each improvement action should name an owner, a due date, and the evidence needed at reassessment.

7. Practical Applications of the Artificial Intelligence Governance Maturity Model

AIGMM may help organizations structure internal assessment and direct resources to capabilities where evidence is weakest. In critical infrastructure, versioned release records, decision logs, escalations, and verified corrective actions from the proposed AIGA workflow can provide evidence for several domains. In healthcare and financial services, assessors could use corresponding clinical or model-risk records while applying the same level criteria to locally defined practices.

Internal comparisons are most interpretable when scope, evidence windows, and rating criteria are comparable. Cross-organization benchmarking requires testing comparability across governance environments and levels of evidence access. Potential effects on resilience, regulatory readiness, decision quality, and stakeholder trust are distinct outcomes that require independent measurement. A maturity rating does not attest to regulatory compliance or guarantee those effects.

8. Future Research Directions

First, assess content coverage with domain specialists and practitioners. Ask whether indicators adequately represent each capability, whether domains overlap materially, and whether the common scoring criteria work across different records and sectors.

Second, conduct independent double-rating of the same evidence packets. Evaluate agreement on the ordered levels and overall rating and report how often insufficient evidence occurs. Weighted agreement statistics and qualitative review of disagreements can reveal unclear criteria, especially at the Defined–Managed boundary. Compare the proposed two-cycle threshold and minimum-domain aggregation with plausible alternatives before adopting any benchmarking rule.

Third, test the rubric in prospective, longitudinal studies within comparable scopes. Examine whether changes in ratings coincide with independently measured changes in decision traceability, verified corrective action, service continuity, or other relevant outcomes. Separately test whether ratings remain comparable across sectors and organizational sizes when sampling and evidence access differ.

9. Limitations

The targeted synthesis is selective. The eight domains, level thresholds, treatment of insufficient evidence, and minimum-domain rule are proposed design choices. The worked example

Vol. 11, No. 06; 2026

ISSN: 2456-3676

illustrates how those choices operate and supplies no estimates of reliability, validity, or organizational effects.

The overall level is sensitive to the lowest-rated domain, so the full profile and assessment scope are essential for interpretation. Differences in record availability, assessment windows, and local responsibilities can affect ratings. The model evaluates governance practices within the reviewed scope. It does not measure AI model quality or establish regulatory conformity.

10. Conclusion

AIGMM proposes a structured way to judge how consistently eight AI governance capabilities are established, managed, and improved. The assessment links each judgment to evidence, retains the full domain profile, and identifies the lowest demonstrated capability as the overall level when every domain is rated. The hypothetical utility assessment shows how the scoring and adjudication procedures work. The contribution is a testable assessment design whose practical value and relationship to organizational outcomes remain to be established.

Authorship Statement

This manuscript represents a collaborative scholarly effort by **Dr. Robb Shawe** and **Dr. Robert W. Clark** and is informed by the complementary foundations of their respective doctoral research programs.

Dr. Robb Shawe served as the lead author and was responsible for the research design, literature synthesis, conceptual integration, development of the **Artificial Intelligence Governance Maturity Model (AIGMM)**, manuscript writing, editing, revisions, formatting, figure development, and preparation of the final manuscript for publication. Dr. Shawe further developed the interdisciplinary theoretical framework by integrating governance science, organizational capability theory, maturity modeling, resilience engineering, socio-technical systems theory, enterprise risk management, explainable artificial intelligence, cybersecurity governance, organizational learning, and adaptive governance into a unified framework for enterprise AI governance maturity.

Dr. Robert W. Clark contributed the foundational subject-matter expertise derived from his doctoral research and extensive professional experience in law enforcement leadership, behavioral threat assessment, intelligence operations, public safety governance, organizational leadership, and critical decision-making. His practitioner insights and conceptual contributions informed the development, refinement, practical applicability, and enterprise implementation considerations of the Artificial Intelligence Governance Maturity Model. Dr. Clark contributed to and reviewed the original manuscript. Both authors accept full responsibility for the originality, scholarly integrity, accuracy, and intellectual content of the published work.

The Artificial Intelligence Governance Maturity Model (AIGMM) represents the original conceptual contribution of this manuscript and was developed through the authors' interdisciplinary synthesis of governance theory, organizational capability theory, maturity

Vol. 11, No. 06; 2026

ISSN: 2456-3676

modeling, enterprise risk management, socio-technical systems theory, and organizational learning.

Statement on Authorship and AI-Assisted Editorial Technologies

The authors developed the original AIGMM, including its eight domains and five levels. They affirm that the intellectual conception, theoretical development, maturity model architecture, analytical reasoning, interpretation of the scholarly literature, interdisciplinary synthesis, governance capability domains, maturity hierarchy, organizational assessment methodology, practical applications, and conclusions presented in this manuscript reflect their original academic scholarship, professional expertise, and collaborative research.

During manuscript preparation, contemporary digital writing and editorial technologies may have been used in a limited capacity to support language refinement, grammatical correction, formatting consistency, organizational structure, and editorial review. These technologies were not used to generate the manuscript's research questions, theoretical foundations, governance maturity framework, governance capability domains, maturity-level architecture, organizational assessment methodology, analytical arguments, practical applications, or scholarly conclusions.
All substantive intellectual contributions—including the development of the Artificial Intelligence Governance Maturity Model (AIGMM), the governance capability domain architecture, the five-level maturity hierarchy, the organizational assessment methodology, and the interdisciplinary theoretical synthesis—were developed by the authors and were critically reviewed, verified, refined, and approved prior to submission.

The authors further acknowledge that contemporary automated AI-authorship detection systems often rely on probabilistic methods that may incorrectly classify highly structured academic writing, conceptual governance frameworks, technical manuscripts, or consistently formal scholarly prose as machine-generated. Such classifications do not constitute evidence of authorship and should not be regarded as definitive indicators of a scholarly manuscript's intellectual origin.

Accordingly, the authors accept full responsibility for the originality, scholarly integrity, and accuracy of this work, as well as for its intellectual contributions. They certify that the manuscript constitutes their independent scholarly contribution to advancing interdisciplinary research in artificial intelligence governance, governance maturity assessment, organizational capability, enterprise risk management, organizational resilience, critical infrastructure governance, cybersecurity governance, and adaptive organizational governance.

Copyright Notice

© 2026 Dr. Robb Shawe and Dr. Robert W. Clark. All Rights Reserved.
This manuscript constitutes an original scholarly work developed through the collaborative integration of the authors' respective doctoral research, professional expertise, and interdisciplinary scholarship. No portion of this manuscript may be reproduced, distributed, transmitted, stored in a retrieval system, or incorporated into derivative works in any form or by

Vol. 11, No. 06; 2026

ISSN: 2456-3676

any means, whether electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the copyright holders, except as permitted under applicable copyright law, fair use provisions, or publisher agreement.

The views and opinions expressed in this manuscript are solely those of the authors and do not necessarily reflect the official positions, policies, or endorsements of any governmental agency, academic institution, employer, professional association, or affiliated organization.

References

Argyris, C., & Schön, D. A. (1978). *Organizational learning: A theory of action perspective*. Addison-Wesley.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management. *Business & Information Systems Engineering, 1*(3), 213–222.

Bevir, M. (2013). *A theory of governance*. University of California Press.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*.

de Bruin, T., Freeze, R., Kulkarni, U., & Rosemann, M. (2005). Understanding the main phases of developing a maturity assessment model. *ACIS 2005 Proceedings*, Article 109. https://aisel.aisnet.org/acis2005/109/

Folke, C., Hahn, T., Olsson, P., & Norberg, J. (2005). Adaptive governance of social-ecological systems. *Annual Review of Environment and Resources, 30*, 441–473.

International Organization for Standardization & International Electrotechnical Commission. (2023). *Information technology—Artificial intelligence—Management system* (ISO/IEC Standard No. 42001:2023). https://www.iso.org/standard/42001

MITRE. (2023). *The MITRE AI Maturity Model and Organizational Assessment Tool guide: A path to successful AI adoption*. https://www.mitre.org/sites/default/files/2023-11/PR-22-1879-MITRE-AI-Maturity-Model-and-Organizational-Assessment-Tool-Guide.pdf

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). *Capability maturity model for software (Version 1.1)* (CMU/SEI-93-TR-024). Software Engineering Institute. https://www.sei.cmu.edu/library/capability-maturity-model-for-software-version-11/

Shawe, R., & Clark, R. W. (2026a). Artificial intelligence governance for critical infrastructure protection: A human-centered conceptual framework. *International Journal of Advanced Engineering and Management Research*.

Shawe, R., & Clark, R. W. (2026b). Operationalizing artificial intelligence governance for critical infrastructure: A governance assurance framework for trustworthy AI in high-consequence environments. *International Journal of Advanced Engineering and Management Research*.

Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509–533.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal getting. *Human Relations, 4*(1), 3–38.

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

Walker, G. H., Stanton, N. A., Salmon, P. M., & Jenkins, D. P. (2008). A review of sociotechnical systems theory. *Theoretical Issues in Ergonomics Science, 9*(6), 479–499.

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology, 54*(12), 1317–1339.

Winter, S. G. (2003). Understanding dynamic capabilities. *Strategic Management Journal, 24*(10), 991–995.