International Journal of Advanced Engineering and Management Research

Vol. 11, No. 06; 2026

ISSN: 2456-3676

Integrated Artificial Intelligence Governance Capability Framework (IAIGCF): Unifying Governance, Assurance, and Maturity for Enterprise AI Excellence

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.2026.11607 URL: http://dx.doi.org/10.51505/ijaemr.2026.11607

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

Abstract
The Integrated Artificial Intelligence Governance Capability Framework (IAIGCF) proposes a way to connect strategic authorization, operational assurance, and maturity assessment to enterprise decisions about AI use. A targeted conceptual synthesis integrates three preceding frameworks into a common review process that links use-case records, assurance findings, capability gaps, risk dispositions, executive decisions, and verified corrective actions. The article compares the design with selected AI risk, management-system, and maturity references, defines candidate governance measures, and uses a published hospital AI study to ground an illustrative application. The illustration demonstrates the proposed handoffs. Independent expert review and prospective organizational testing are required to assess feasibility, reliability, and effects.

Keywords: artificial intelligence governance, enterprise governance, governance integration, governance assurance, governance maturity, organizational capability, enterprise risk management, adaptive governance, organizational resilience

1. Introduction

Executive leaders need to know whether the controls they authorize for AI use operate as intended, whether the organization can sustain them, and what action is warranted when evidence falls short. A risk register, an assurance report, and a maturity assessment can each answer part of that question. Their value for enterprise decisions depends on whether findings can be traced to the relevant use cases, accountable owners, and verified actions.

Article 1 introduces the Artificial Intelligence Governance Framework for Critical Infrastructure (AIG-CI), which specifies authority and governance checkpoints (Shawe & Clark, 2026a). Article 2 proposes the Artificial Intelligence Governance Assurance (AIGA) Framework, which produces evidence about decisions and controls in operation (Shawe & Clark, 2026c). Article 3 proposes the Artificial Intelligence Governance Maturity Model (AIGMM), which assesses sustained capability across eight domains within a defined organizational scope (Shawe & Clark, 2026b). Article 4 integrates their outputs into an enterprise review and corrective-action process.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

The guiding question is how an organization can translate operational assurance evidence and maturity findings into a traceable executive decision and verify that the decision was carried out. IAIGCF is a conceptual answer to that question.

2. Literature Review

2.1 Governance, Assurance, and Capability

In this framework, governance sets the authorized scope and decision rights. Assurance examines specific decisions, controls, or exceptions. Maturity assessment examines whether the responsible practices are established, repeated, measured, and adapted across the assessment scope. Research on organizational capability and maturity supports distinguishing a documented rule, evidence of repeated use, and evidence of verified change (Becker et al., 2009; Teece et al., 1997; Winter, 2003).

2.2 Comparison with Existing Approaches

Table 1 compares the scope, outputs, and implications of three relevant approaches for the proposed IAIGCF design.

Table 1. Comparison with Existing AI Governance Approaches

Approach	Scope and output	Relationship to IAIGCF
NIST AI RMF 1.0	Voluntary AI risk-management outcomes and actions organized under Govern, Map, Measure, and Manage.	IAIGCF uses risk identification, measurement, and disposition to connect evidence from its component models to a documented executive decision.
ISO/IEC 42001:2023	Requirements for an organizational AI management system and its continual improvement.	The proposed records could support management review. Assessing management-system conformity requires a separate evaluation.
MITRE AI Maturity Model	Enterprise AI adoption assessment that includes governance and responsible use.	IAIGCF uses the AIGMM governance profile as one input to enterprise disposition and tracks whether the resulting action was verified.
IAIGCF (proposed)	Enterprise governance integration through linked records and accountable handoffs.	Combines use-case authorization, event-level assurance, scope-level maturity, and risk disposition in a cycle of review and verified action.

Note. The comparison uses the published NIST AI RMF, ISO/IEC 42001 description, and MITRE assessment guide (ISO/IEC, 2023; MITRE, 2023; Tabassi, 2023). It compares conceptual scope and outputs.

The comparison shows substantial overlap in risk ownership, performance evaluation, and improvement. IAIGCF's proposed contribution is the explicit transfer of records between the three Series III models and enterprise review. A reviewer can trace a control exception through risk disposition, an accountable executive decision, and verification of the resulting action. This is a design contribution. Comparative effectiveness and conformity require separate evaluation.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

3. Theoretical Foundations of the Integrated Artificial Intelligence Governance Capability Framework (IAIGCF)

Governance theory informs the assignment of decision rights and accountability, while organizational capability theory informs the distinction between one instance of compliance and a practice that persists across units and over time (Bevir, 2013; Teece et al., 1997; Winter, 2003). Enterprise risk management (ERM) provides the common record for translating assurance findings into risk priorities, dispositions, and resource decisions (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017).

Socio-technical systems theory informs the requirement to review technical evidence alongside staff authority, workload, and real workflow execution (Trist & Bamforth, 1951; Walker et al., 2008). Resilience engineering informs monitoring, restriction, and fallback under changing conditions (Hollnagel, 2014). Organizational learning and adaptive governance inform verification of corrective action and revision of authorization or policy when circumstances warrant it (Argyris & Schön, 1978; Folke et al., 2005).

4. Integrated Framework Development Methodology

4.1 Research Design and Source Selection

IAIGCF is a conceptual integration of Articles 1–3, supported by a targeted narrative synthesis. Sources were selected for their direct relevance to at least one design problem: identifying who holds decision authority, determining what evidence demonstrates practice or capability, or explaining how findings lead to adaptation. Governance and organizational scholarship informed the constructs in Section 3. NIST AI RMF, ISO/IEC 42001, and MITRE were selected as published comparators representing risk management, management-system requirements, and enterprise maturity assessment, respectively. The source set is purposive, and its coverage is selective. The comparison focuses on documents that describe enterprise duties or assess organizational capability. Model benchmarks and sector-specific technical checklists are outside the scope of the comparison.

4.2 Construct Identification and Integration

The comparative procedure can be followed by recording each source's purpose, assessment unit, and principal output. For each construct, identify the accountable role, the record it produces, the receiving process, and the decision that record supports. For example, authorization travels from strategic governance to operations as a use-case record, while a documented exception travels from assurance to the risk owner for disposition. Similar responsibilities are consolidated by decision authority. Assurance and maturity remain distinct because a decision record and a scope-wide capability rating answer different questions.

Table 2 records the resulting handoffs. A shared use-case identifier links the authorization, decision, and exception records, and relevant risk and action items. A maturity finding additionally carries its assessment scope and evidence window because it can refer to multiple use cases. ERM and executive review reconcile priorities and assign a decision owner, action owner, and verification requirement.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

4.3 Conceptual Coherence and Validation Status

The conceptual check asks whether each output has a receiving role, whether the record is sufficient for the proposed decision, and whether the resulting action can be independently verified. The worked application in Section 6 traces a finding through this sequence and identifies what evidence an operator would need. Independent expert evaluation, organizational implementation studies, and empirical tests of effectiveness remain future work.

5. Integrated Artificial Intelligence Governance Capability Framework (IAIGCF)

5.1 Enterprise Architecture

IAIGCF links strategic authorization, operational assurance, and scope-level maturity assessment to enterprise risk and executive review. The executive decision records the rationale for continued use, restriction, remediation, or retirement. The action record captures what changed and how it was verified.

Figure 1 shows the outputs of the three frameworks and where they enter enterprise review.

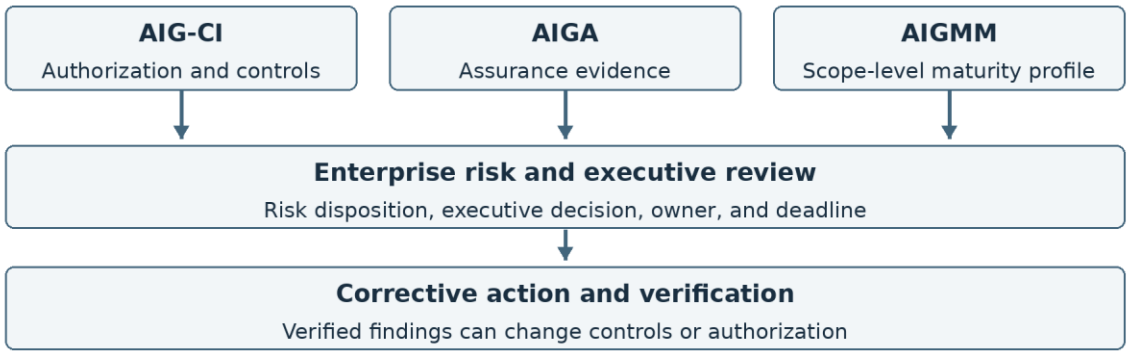


Figure 1. Integrated Artificial Intelligence Governance Capability Framework

Note. Authors' conceptual architecture. The three inputs have different units of analysis. A maturity profile may cover multiple use cases and should retain its organizational scope.

The shared records allow executives to ask whether an exception concerns one decision or signals a capability gap. Table 2 identifies the roles that pass and receive that evidence.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

Table 2 traces each Series III framework's contribution to the next accountable decision.

Table 2. Evidence Handoffs Across the Shawe–Clark Series III

Series III framework	Output passed forward	Receiving role and decision
Article 1: AIG-CI	Use-case authorization, delegated authority, controls, and evidence requirements.	Service owner implements the workflow and routes relevant events to assurance.
Article 2: AIGA	Decision and control records, exceptions, local performance evidence, and corrective actions.	Assurance and risk leads assess control exceptions. The maturity assessment lead checks evidence coverage and recurrence.
Article 3: AIGMM	Eight-domain profile, scope, evidence window, and overall level when all domains can be rated.	Risk owner distinguishes a one-off failure from a capability gap and proposes a disposition.
Article 4: IAIGCF	Executive decision, risk disposition, action assignment, deadline, and closure criteria.	Service owner implements the decision. A designated reviewer verifies closure. Sponsor revisits authorization when required.

Note. The roles are proposed defaults. Organizations should assign equivalents based on their delegated authority and operating structure.

A verified corrective action can change operating instructions or the approved scope. Figure 2 shows how that change enters the next cycle.

5.2 Enterprise Governance Lifecycle

Figure 2 connects authorization, implementation, assurance, maturity assessment, executive disposition, and verified adaptation in six phases.



Figure 2. Enterprise Artificial Intelligence Governance Lifecycle

Note. ERM operates throughout the cycle. Phase 5 is the formal review and disposition decision. Urgent exceptions may trigger escalation as soon as they are identified.

Each phase produces evidence for the next accountable role. Section 6 uses the same six phases to show how a bounded implementation can proceed.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

5.3 Governance Performance Measures

Table 3 defines candidate indicators for whether the enterprise handoffs occur, documented decisions use the available evidence, and corrective actions close on time.

Table 3. Candidate Enterprise Governance Measures

Indicator	Definition	Record and owner	Review and response
Decision traceability	Consequential AI-supported actions with retrievable source evidence, version, human authorization, rationale, and disposition ÷ qualifying actions in the window.	Action and decision logs. Assurance lead.	Monthly. Escalate each missing material record.
Timely risk disposition	Material findings due in the window with a documented risk disposition by the approved deadline ÷ material findings due.	Risk register. Risk owner.	Monthly. Escalate overdue material items under local rules.
Executive evidence use	Reviewed executive dispositions with links to relevant assurance evidence and the available maturity findings or a documented evidence gap ÷ dispositions reviewed.	Executive decision register. Governance lead.	Quarterly. Return incomplete records for review.
On-time verified closure	Actions due in the window with closure independently verified on or before the approved deadline ÷ actions due.	Corrective-action register. Assurance lead.	Monthly. Retain overdue items as open and escalate by risk.

Note. Record numerators and denominators for each reporting window. A zero denominator is not applicable. Record unknown eligibility or missing evidence separately. Review intervals and response criteria are proposed for local approval.

Before a pilot, specify which cases and events qualify, who owns each source record, and which deviations require immediate review. Reconcile the registers at each reporting cutoff and examine material exceptions even when aggregate rates meet expectations. Measure the burden of operating the process alongside evidence coverage. Scope-level maturity remains the eight-domain profile and, when available, the overall level defined by AIGMM.

6. Enterprise Implementation and Organizational Applications

6.1 Bounded Implementation

Start with one bounded set of related, material-risk AI use cases. Assign an executive sponsor, service owner, assurance lead, maturity assessment lead, risk owner, and an independent verifier or other designated reviewer. Reuse the organization's existing authorization, risk, and corrective-action registers where they preserve identifiers, version history, and decision ownership.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

6.2 Phase 1: Strategic Direction

The sponsor approves the use-case boundary, delegated authority, evidence requirements, risk limits, and fallback. Record conditions that require immediate restriction or a new authorization.

6.3 Phase 2: Implementation

The service owner embeds operating and review requirements in the workflow. Confirm that staff can apply and document the controls, use the fallback, and escalate exceptions.

6.4 Phase 3: Assurance

The assurance lead reconciles decision, action, and exception records for the reporting window. Route material findings to the risk owner promptly. Preserve the underlying records for independent review.

6.5 Phase 4: Maturity Assessment

The assessment lead evaluates the evidence across the defined scope and reports the eight AIGMM domain ratings. When all eight can be rated, the overall level is the lowest supported level. When evidence is insufficient for any domain, withhold the overall level and identify the evidence needed.

6.6 Phase 5: Risk and Executive Review

The risk owner evaluates material findings against local tolerances, explains alternative dispositions, and forwards the evidence to the authorized executive. The executive records the decision, rationale, owner, completion deadline, and required proof of closure. Unresolved high-consequence risk is handled under the organization's escalation and fallback rules.

6.7 Phase 6: Verified Adaptation

The action owner implements the approved change. A designated reviewer checks the agreed evidence for closure and records unresolved gaps. If scope, controls, or delegated authority change materially, the sponsor revisits the authorization before wider use.

6.8 Worked Application: Hospital AI Governance

Wong et al. (2026) evaluated an updated proprietary sepsis prediction model across four health systems. The study reported better discrimination than the original model alongside substantial variation across institutions and a high alert burden. Article 2 uses this evidence to illustrate local assurance. The example below extends that use to enterprise review. The governance records, counts, decisions, and actions described here are hypothetical and do not describe the study sites.

Consider a hospital that has authorized a bounded alert pilot. During a monthly review, the assurance lead finds that only 18 of 20 consequential AI-supported actions have reconstructable records. The action log confirms that two actions occurred. Their missing records prevent verification of the rationale and human authorization. The assurance lead calculates traceability as 18 ÷ 20 (90%) and forwards both exceptions to the risk owner. The maturity assessment

Vol. 11, No. 06; 2026

ISSN: 2456-3676

documents an operational integration gap and withholds an overall level because the case evidence does not support ratings for all eight domains.

The executive sponsor restricts expansion, directs the service owner to correct the record capture process, and requires the approved fallback if the pilot cannot operate within its authorization. At the reporting cutoff, one of two actions due that month was independently verified by its approved deadline, so on-time verified closure is 50%. The remaining action stays open. In this illustration, expansion is reconsidered after the outstanding action is verified and a new review confirms that covered actions can be reconstructed. This example shows how assurance findings, maturity evidence, executive disposition, and closure checks can be linked through the same scope and use-case records.

6.9 Transfer Across Sectors

A utility, financial institution, or public agency could use the same record relationships with locally defined decisions, regulatory duties, and evidence. Gains in resilience, regulatory readiness, stakeholder trust, or decision quality are hypotheses requiring separate measures and evaluation.

7. Future Research Directions

Independent experts in AI governance, operations, risk, and assurance should review the proposed handoffs and rate their clarity, completeness, and feasibility. Give reviewers the same records and ask them to identify the accountable role, the appropriate escalation route, and the evidence required for closure. Document initial agreement, recurring disagreements, and revisions to the model.

A prospective pilot could compare the existing process with the integrated process using the same eligibility rules and observation windows, or a staggered rollout where comparable units are available. Primary outcomes could include decision traceability, timely risk disposition, and independently verified corrective action. Track review burden, delayed decisions, and service continuity alongside those outcomes. Record concurrent changes in staffing, policy, or model version and examine whether they affect interpretation.

Cross-sector studies should assess whether the same evidence and decision relationships remain workable under different regulations and resources. Test consistency of record classification and maturity assessment before cross-organization benchmarking. Assess resilience, regulatory readiness, and stakeholder trust separately if they are proposed outcomes.

8. Limitations

IAIGCF is a conceptual design based on a purposive synthesis. The comparison is selective, the candidate indicators are unvalidated, and the worked application illustrates the mechanics of the proposed integration. It does not establish that the framework is effective or that participating institutions used it.

What can be assessed depends on local authority, access to evidence, the scope of each maturity assessment, and the capacity to verify action. Indicator values may reflect differences in

Vol. 11, No. 06; 2026

ISSN: 2456-3676

documentation or workload. Findings should be interpreted alongside operating outcomes and applicable requirements.

9. Conclusion

IAIGCF connects strategic authorization, operational assurance, and scope-level maturity findings to enterprise risk review, executive disposition, and verified corrective action. Its contribution is a proposed design for tracing the records and decisions through that cycle. The next empirical question is whether independent reviewers and operators can use the design reliably and whether it improves traceability and closure under routine conditions.

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 **Integrated Artificial Intelligence Governance Capability Framework (IAIGCF)**, manuscript writing, editing, revisions, formatting, figure and table development, and preparation of the final manuscript for publication. Dr. Shawe further developed the interdisciplinary theoretical framework by integrating governance systems theory, organizational capability theory, governance assurance, governance maturity modeling, resilience engineering, socio-technical systems theory, enterprise risk management, organizational learning, adaptive governance, explainable artificial intelligence, and cybersecurity governance into a unified enterprise governance architecture.

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, implementation strategy, and enterprise governance considerations of the Integrated Artificial Intelligence Governance Capability Framework. 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 **Integrated Artificial Intelligence Governance Capability Framework (IAIGCF)** represents the original conceptual contribution of this manuscript and synthesizes the complementary governance concepts developed throughout the Shawe–Clark Series III into a unified enterprise governance architecture. The framework integrates strategic governance, governance assurance, governance maturity, enterprise risk management, organizational learning, resilience engineering, socio-technical systems theory, and adaptive governance into a comprehensive enterprise capability supporting trustworthy artificial intelligence, organizational resilience, and continuous governance improvement.

Vol. 11, No. 06; 2026

ISSN: 2456-3676

Statement on Authorship and AI-Assisted Editorial Technologies

The authors developed the original IAIGCF and its three predecessor frameworks. They affirm that the intellectual conception, theoretical development, enterprise governance architecture, analytical reasoning, interpretation of the scholarly literature, interdisciplinary synthesis, integrated governance capability framework, implementation methodology, enterprise governance lifecycle, practical applications, and conclusions presented in this manuscript are the result of 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, enterprise governance architecture, integrated governance framework, implementation methodology, analytical arguments, organizational applications, or scholarly conclusions.

All substantive intellectual contributions—including the development of the Integrated Artificial Intelligence Governance Capability Framework (IAIGCF), the enterprise governance integration architecture, the enterprise governance lifecycle, the implementation methodology, and the interdisciplinary theoretical synthesis—originated with 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 employ probabilistic methodologies 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 this manuscript constitutes their independent scholarly contribution to advancing interdisciplinary research in artificial intelligence governance, enterprise governance integration, governance assurance, governance maturity, organizational capability, enterprise risk management, resilience engineering, organizational learning, cybersecurity governance, critical infrastructure governance, and adaptive enterprise 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 any means, whether electronic, mechanical, photocopying, recording, or otherwise, without the

Vol. 11, No. 06; 2026

ISSN: 2456-3676

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*.

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

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. Ashgate.

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

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). Artificial intelligence governance maturity model (AIGMM): A capability-based framework for organizational assessment, continuous improvement, and trustworthy AI. *International Journal of Advanced Engineering and Management Research*.

Shawe, R., & Clark, R. W. (2026c). 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.

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. https://doi.org/10.1177/001872675100400101

Vol. 11, No. 06; 2026

ISSN: 2456-3676

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.

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

Wong, A., Currey, D., Schwinne, M., Park-Egan, B., Meyer, S., Gutting, A., Cao, J., Khan, S., Dantes, R., Pan, T., Buchman, T., Singh, K., Bhavani, S. V., Lyons, P. G., Sjoding, M. W., & Tarabichi, Y. (2026). Multicenter prospective validation of an updated proprietary sepsis prediction model. *JAMA Network Open, 9*(2), e260181. https://doi.org/10.1001/jamanetworkopen.2026.0181