

The Digital Operations System

The management infrastructure for Digital Labor

Fabio A. Thiers, MD, PhD

ConverGen AI, New York, NY, USA

ABSTRACT

Digital Operations becomes necessary when AI begins performing accountable work within an organization. Even if a healthcare entity manages AI governance, cybersecurity, model assessment, procurement, workflow automation, and compliance, it may still lack the essential system for daily Digital Labor operation. The Digital Operations System (DOPs) serves as the management framework linking role design, context, identity, access, control, supervision, telemetry, autonomy, incident review, learning, risk, and portfolio governance. This article describes DOPs as the operational layer for Digital Workers, which enables Digital Labor to be visible, bounded, measured, supervised, improved, and reversible.

Keywords: healthcare AI; Digital Operations; Digital Operations System (DOPs); Digital Workers; Digital Labor; AI governance; Human-Digital Organizations; organizational context; managed autonomy; operational telemetry; AI operations; risk management.

Key points

- **AI governance is necessary but insufficient once AI performs accountable work.** Governance determines whether AI should be used; Digital Operations manages how Digital Workers perform authorized work safely, consistently, and under institutional accountability.
- **Digital Workers require a management system.** DOPs provides the operational infrastructure through which Digital Workers are created, supplied with organizational context, supervised, measured, improved, and retired throughout their lifecycle.
- **Operational evidence enables reliable Human-Digital Organizations.** By connecting role definition, context, authority, supervision, telemetry, incidents, and learning, DOPs allows human and digital work to operate together within accountable workflows.
- **Digital Operations creates the information needed to manage enterprise risk.** The operational records generated through DOPs support organizational learning while providing evidence for governance, quality management, risk management, financial planning, and ultimately business insurance underwriting.

AI governance is necessary but incomplete

AI governance asks essential questions. Which uses are acceptable? Which risks require review? Which policies apply? Which vendors meet organizational expectations? Which fairness, privacy, safety, security, and transparency standards should be met? These questions matter, and recognized AI risk and management frameworks provide useful structure.¹⁻³

But governance alone does not operate work. A committee can approve a prior-authorization Digital Worker without providing current payer-policy context, configuring least-privilege access, designing escalation procedures, measuring reviewer burden, logging tool calls, classifying near misses, or deciding whether to narrow authority after a policy change. Those tasks are not peripheral. They are the operating system of Digital Labor.

The pattern is historically familiar. Quality management, patient safety, and information security each became management disciplines when complex work could no longer be made reliable

through individual craft, after-the-fact inspection, or scattered technical controls.^{4,5} Digital Labor is entering the same sequence: new capability creates operational complexity, complexity creates risk, and risk creates the need for management. This is the gap Digital Operations fills. It begins where AI moves from product capability into institutional work.

Digital Operations becomes necessary when Digital Workers perform accountable work

Healthcare organizations are beginning to see the need to manage Digital Workers, which are more than an abstract AI capability. They are characterized as bounded operational roles through which AI performs accountable work under organizational authority. Managing Digital Labor therefore requires more than supervising models or workflows. It requires managing the operational roles through which work is delegated, supervised, measured, and continuously improved. DOPs provides the management infrastructure for those roles rather than for the underlying models alone.

A Digital Worker can touch many domains at once. It may use a model from one vendor, a retrieval index maintained by another team, a credentialed account in an EHR, a payer portal, a document management system, a human review queue, and a compliance policy. It may affect revenue, patient communication, clinical documentation, privacy, and operational performance.

No single traditional function owns all of that. IT can manage infrastructure but may not own payer-policy accuracy. Compliance can define boundaries but may not manage queue performance. Clinical leadership can define review standards but may not maintain identity controls. Operations can own the workflow but may not monitor model drift or the distinctive security risks that agentic systems introduce around goals, tools, identity, privilege, and cascading failure.⁶ Procurement can negotiate vendor terms but cannot supervise daily execution.

Digital Operations is the cross-functional discipline that connects these pieces around work. It makes the Digital Worker visible as a managed role rather than a hidden technical capability. Without that visibility, shadow Digital Workers become the operational equivalent of unauthorized contractors holding production credentials.

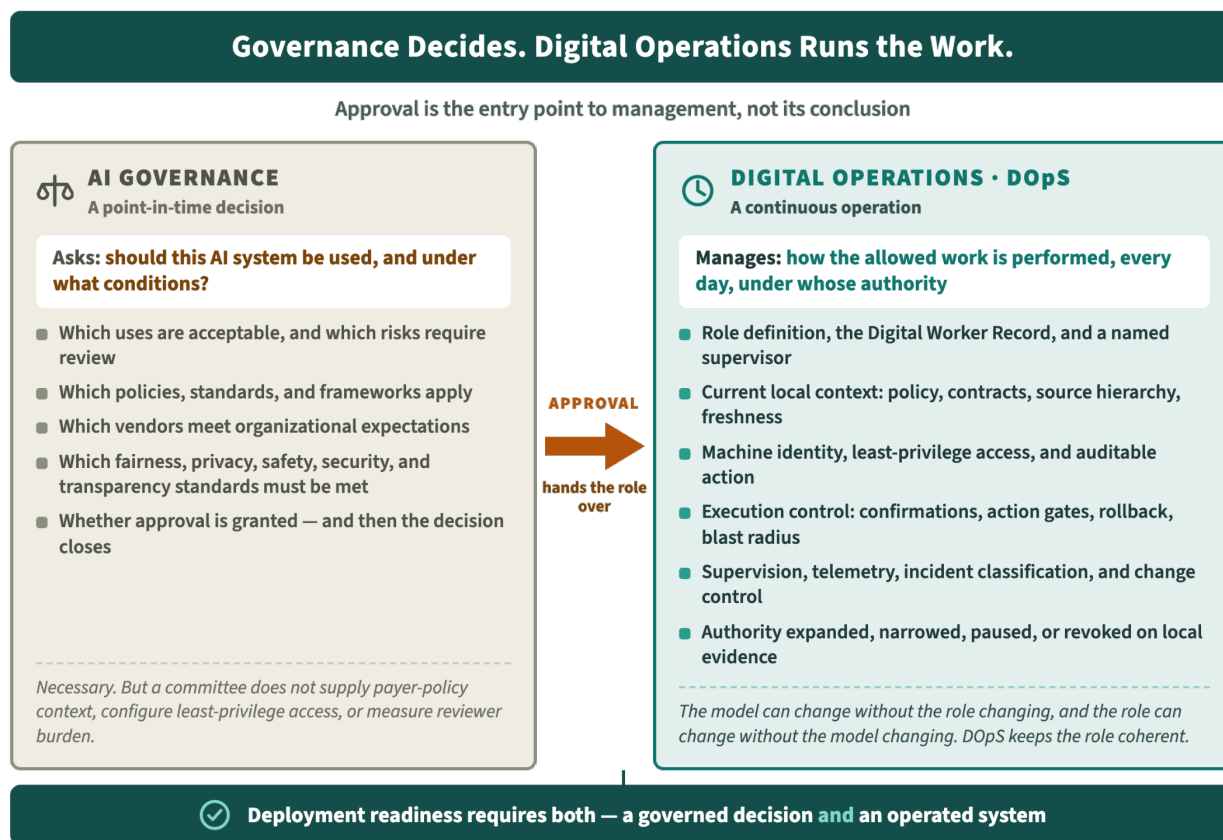


FIGURE 1 - DOPs versus AI governance. Governance decides whether an AI system should be used and under what conditions; DOPs manages the allowed work every day. Approval is the entry point to management, not its conclusion, and deployment readiness requires both.

DOPs is the operating system of Digital Labor

Every management discipline eventually develops a management system. Quality management systems, information security management systems, and, more recently, AI management systems all reflect the same institutional pattern: the system does not replace judgment; it makes judgment repeatable, and it does not remove accountability; it makes accountability operational.^{2,5}

DOPs can be understood in these terms as the operating system for Digital Labor. It brings together the familiar processes historically used to build and manage a human workforce, enabling the creation, authorization, contextualization, access, supervision, measurement, improvement, suspension, and retirement of Digital Workers.

The DOPs role is also to readily answer practical questions: Which Digital Workers exist? What are they allowed to do? Which systems can they access? Which context sources are authoritative? What evidence do they preserve? Who supervises them? What incidents have occurred? Which autonomy level is currently justified? Which worker depends on which model, vendor, policy source, portal, or human review queue?

Without an integrated system that can promptly provide these answers, the organization's management cannot effectively control instances of Digital Labor that work technically but lack the traceability needed for enterprise management, scalable deployment, and future risk financing.

Core DOPs components

The core components of DOPs should be designed as operating capabilities rather than static policy documents:

- The **registry** records every Digital Worker and its role, owner, supervisor, systems, access, autonomy band, validation status, incidents, and lifecycle.
- The **context layer** manages the local knowledge required for work: policies, contracts, source hierarchy, workflow rules, patient and case facts, partner-system reliability, and freshness.
- The **identity and access layer** gives controlled permissions and auditable actions to each worker.
- The **execution-control layer** governs tool use, confirmations, action gates, rollback, and blast-radius limits.
- The **supervision layer** defines human review, escalation, approval, override, correction, and coaching; it must make review meaningful rather than ceremonial, because decision support can introduce new errors when reviewers over-rely on system outputs or cannot see the basis for a recommendation.^{7,8}
- The **telemetry and evidence layer** captures inputs, sources, tool calls, decisions, outputs, approvals, actions, outcomes, and corrections.
- The **incident-review layer** classifies failures, near misses, context gaps, tool errors, and escaped material errors.
- The **change-control layer** determines which model, prompt, policy, portal, or workflow changes require revalidation, temporary narrowing of authority, or compliance review.
- The **autonomy-management layer** expands, narrows, pauses, or revokes authority based on evidence.
- The **learning layer** turns reviewed traces into updated context, workflow changes, worker improvements, and organizational memory, which is the mechanism through which Digital Labor can serve the aims of a Learning Health System.⁹

The registry is most useful when implemented through a persistent Digital Worker Record that follows each role throughout its lifecycle. Rather than documenting only technical configuration, the record connects role definition, operational identity, authority, supervision, context, evidence, incidents, performance, and retirement into a single institutional object. This continuity allows organizations to improve Digital Workers over time even as underlying models, tools, vendors, and workflows evolve.

These components are interconnected rather than standalone modules. Role design dictates the necessary permissions; permissions specify the evidence to be gathered; evidence influences whether autonomy should grow; autonomy determines the supervision needed; supervision leads to corrections; and corrections update the context. DOpS is the system that maintains these connections, ensuring Digital Labor remains governable instead of just being instrumented.

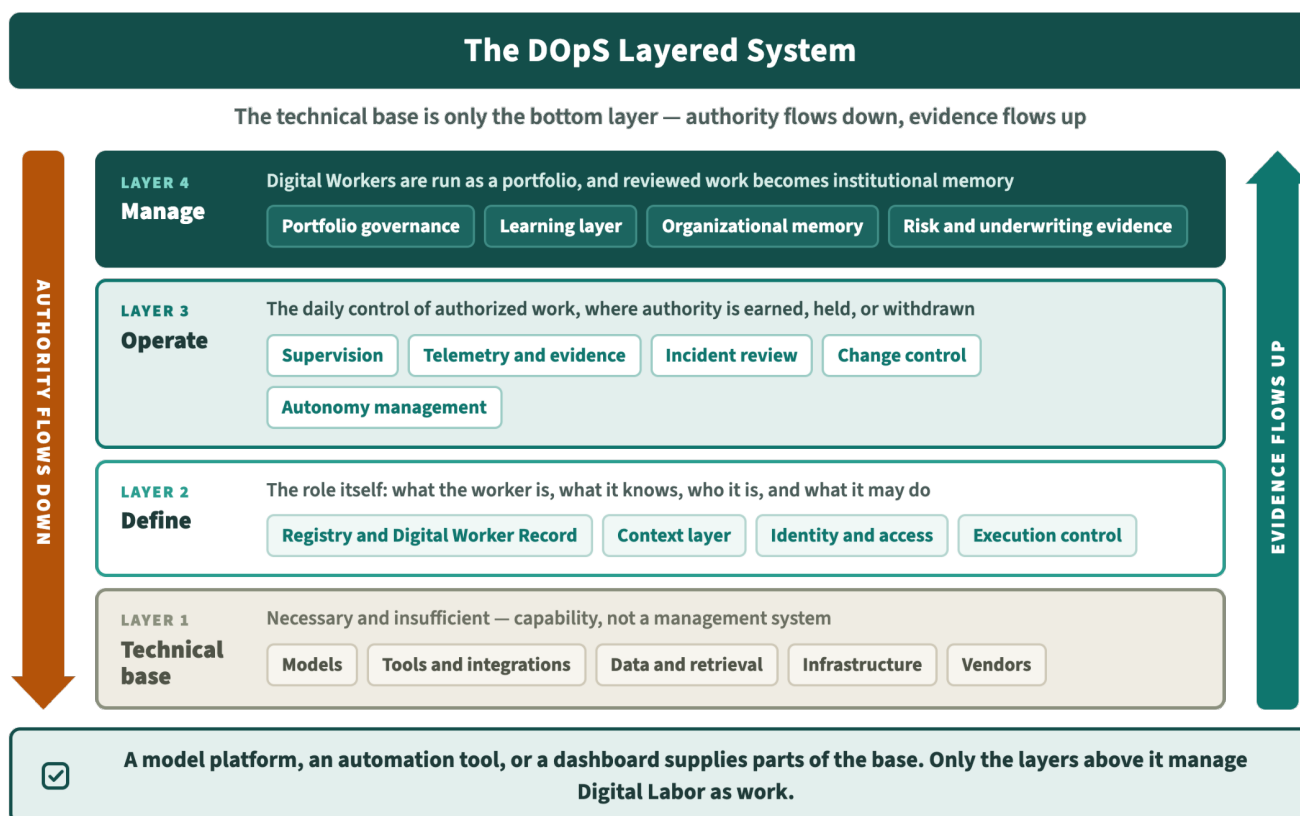


FIGURE 2 - DOpS layered system. The technical base is only the bottom layer; above it, DOpS defines roles, context, identity, and execution control, operates supervision, telemetry, autonomy gates, change control, and incident response, and manages the portfolio. Evidence flows up the stack while authority flows down.

DOpS must be cross-functional

Digital Labor crosses departmental boundaries, so Digital Operations cannot live entirely inside innovation, IT, compliance, or clinical operations. A Digital Worker preparing authorization packets may require clinical leadership to define medical review thresholds, operations to define workflow, revenue cycle to define outcome metrics, IT to manage identity and integrations, security to define access controls, compliance to define evidence retention, legal to review vendor responsibilities, and quality/risk to define incident categories.

Cross-functionality should not imply scattered ownership. Each Digital Worker must have a designated operational owner and supervisor. DOpS offers the shared infrastructure and management processes, while local owners are still responsible for their role's tasks. This approach is similar to cybersecurity, quality, and clinical safety, which rely on enterprise frameworks combined with local accountability. A related idea is that organizations may utilize external platforms, models, and integrators, but they cannot delegate accountability for the Digital Labor functioning within their environment, just as they cannot delegate responsibility for quality or security.

The healthcare safety literature's sociotechnical framing is useful here: outcomes emerge from interactions among people, tasks, tools, technologies, organization, and environment.¹⁰⁻¹² Digital Labor intensifies that interaction because AI systems can act across the same surfaces humans use.

DOpS is not a model platform or automation tool

A model platform helps select, host, evaluate, route, or monitor models. An automation tool executes workflow steps. A governance process approves or constrains use. An observability dashboard shows what happened. DOpS is different. It manages Digital Labor as work, and it connects what happened to authority, context, accountability, and learning.

This distinction matters because the Digital Worker may use several models, several tools, and several policies over time. The model can change without the role changing. The role can change without the model changing. The workflow can change because a payer portal changes. The context can change because an internal policy is updated. The supervisor can change because the operating team is reorganized. DOpS is the layer that keeps the role coherent across these changes. For the same reason, the system should be model-agnostic: new models should enter as

controlled components that are validated locally against the role, because performance in one setting does not guarantee performance under another organization's data, workflows, and patients, and behavior can shift as local conditions change.^{13,14}

MLOps, software-engineering practice, model cards, dataset datasheets, and audit frameworks all contribute important pieces.^{15–21} DOPs builds on them but adds the management of role-bearing work under local institutional authority. DOPs therefore supports the complete operational lifecycle of Digital Workers—from creation and local configuration through supervision, operational improvement, managed autonomy, and retirement. Its purpose is not simply to deploy AI capabilities but to enable organizations to build, operate, and continuously improve Digital Labor under institutional control.

The maturity path

A practical maturity path begins with visibility. The organization should know where AI-enabled systems are performing or materially shaping work. The next stage is role definition: each

Digital Worker has a record, owner, supervisor, scope, access profile, and evidence requirements. The third stage is controlled execution: context, permissions, supervision, telemetry, and incident review operate consistently. The fourth stage is evidence-gated authority: autonomy expands or narrows by function based on local performance. The fifth stage is portfolio governance and learning: Digital Workers are managed as operating capacity, and work traces improve the organization.

Maturity should not be measured by the number of autonomous agents. A more useful measure is the percentage of digital work that is visible, role-defined, context-supplied, access-controlled, supervised, measurable, incident-reviewable, and reversible.

This maturity path also supports external accountability. Regulatory, security, privacy, and health IT requirements increasingly emphasize safeguards, transparency, monitoring, and reviewability.^{22–27} DOPs provides the organization with an execution structure for those expectations without reducing Digital Labor to mere compliance documentation.

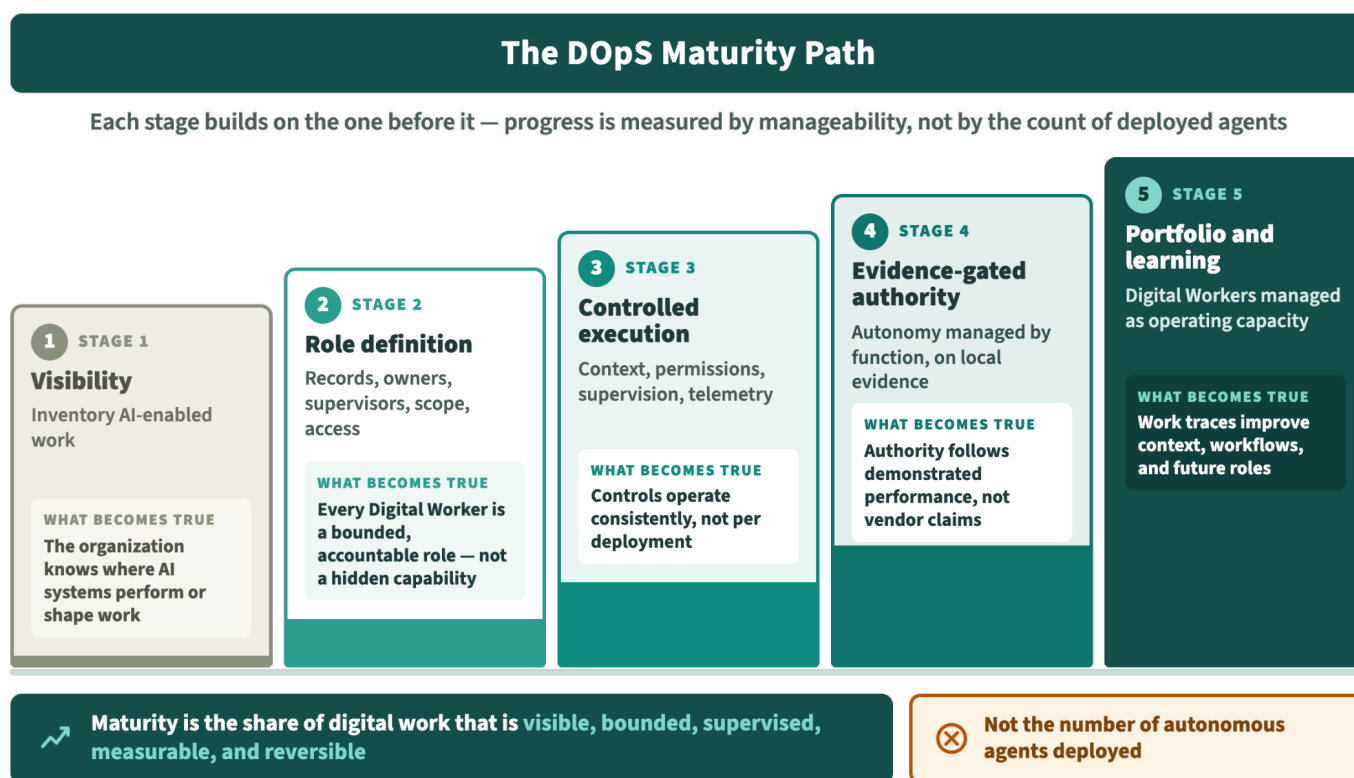


FIGURE 3 - DOPs maturity path. Each stage builds on the previous one; progress is measured by the manageability of digital work, not the count of deployed agents.

The executive test

The state of Digital Operations can be assessed directly. Each row below names a domain, the question an executive should be able to ask, and the evidence a functioning DOPs would produce in minutes rather than meetings.

Close: Digital Operations is how Digital Labor becomes manageable

Digital Operations is not another layer of bureaucracy. It is the management system required when AI begins performing accountable work. Without it, an organization may have impressive pilots, strong models, useful automations, and good

intentions, yet still lack visibility into role scope, context, authority, supervision, evidence, incidents, and lifecycle.

The practical executive question is straightforward: if Digital Workers entered ten workflows tomorrow, could the organization say which workers exist, what they are allowed to do, what context they use, who supervises them, what actions they took, what errors occurred, and whether authority should change?

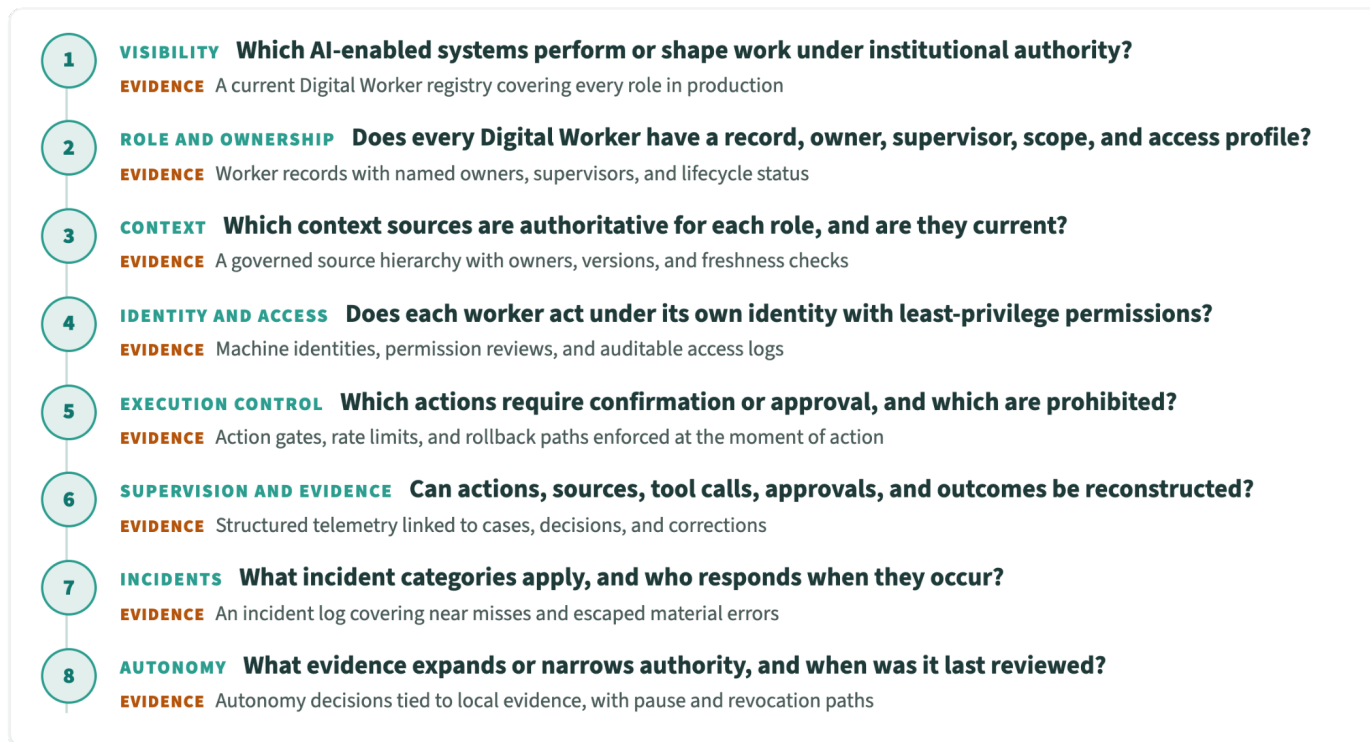
If the answer is no, the organization does not yet have Digital Operations. It has deployments. The difference is not the sophistication of the models. It is the presence of a management system that makes Digital Labor visible, bounded, supervised, evidenced, and reversible — and that makes every subsequent Digital Worker easier to manage than the last.

As Digital Operations matures, organizations are likely to develop enduring capabilities for creating, operating, supervising, and continuously improving Digital Workers, much as they previously developed capabilities for quality, cybersecurity, and information security. Rather than treating AI deployments as isolated technology projects, Digital Operations provides the institutional framework through which Digital Workers become a managed operational workforce integrated with human teams.

The operational information generated through DOpS also extends beyond day-to-day management. Persistent Digital Worker Records preserving role definition, authority, supervision, performance, incidents, and operational history create evidence that supports organizational learning while making Digital Labor more observable as an operational risk. As digital work becomes economically significant, these evidence structures may also support more consistent risk management, risk pricing, and ultimately business insurance underwriting for Digital Labor.

The Executive Test for Digital Operations

Eight questions a functioning DOpS answers in minutes rather than meetings



✓ A deployment becomes a managed operation when every row can be answered from the system of record

FIGURE 4 - Executive test for Digital Operations Systems. All answers should be immediately available to healthcare managers.

Glossary of key concepts

- **Digital Operations.** The management discipline for designing, supervising, measuring, governing, and improving Digital Labor.
- **DOpS.** The system or platform layer that implements Digital Operations across Digital Worker roles.
- **Digital Worker.** An AI-enabled system that performs a bounded, supervised role within an organization's workflows under institutional authority.
- **Digital Worker registry.** The institutional inventory of Digital Workers, roles, owners, systems, access, authority, evidence, and lifecycle status.
- **Digital Worker Record.** The persistent institutional record that defines and maintains a Digital Worker's role, ownership, operational identity, authority, context, supervision, evidence, performance, incidents, organizational memory, and lifecycle.

- **Execution control.** The rules and technical mechanisms that govern tool use, permissions, confirmations, action gates, rollback, and logging.
- **Autonomy management.** Evidence-based expansion, narrowing, pause, or revocation of digital-worker authority by function.
- **Change control.** The process that determines which model, prompt, policy, portal, or workflow changes require revalidation, temporary narrowing of authority, or compliance review.

Live Article information

This PDF is a dated snapshot of a continuously maintained Live Article. Material updates undergo editorial review, and substantive public revisions are released when warranted.

The current maintained article and evidence base are available through the ConverGen Digital Operations Advisor: www.convergen.ai/advisor/

Peer-review status: This public edition has not undergone external peer review.

Competing interests: The author is the founder and CEO of ConverGen AI, which develops and commercializes a Digital Operations System (DOPs) for healthcare organizations.

AI-assisted tools: AI-assisted tools supported research synthesis, drafting, editing, and figure production. The author reviewed and takes responsibility for all content.

Author ORCID: 0009-0008-1814-1983.

References

1. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1 (2023). doi:10.6028/NIST.AI.100-1.
2. International Organization for Standardization. ISO/IEC 42001:2023 Artificial intelligence – Management system (2023). <https://www.iso.org/standard/81230.html>. Accessed 30 Jun 2026.
3. International Organization for Standardization. ISO/IEC 23894:2023 Artificial intelligence – Guidance on risk management (2023). <https://www.iso.org/standard/77304.html>. Accessed 30 Jun 2026.
4. Institute of Medicine. To Err Is Human: Building a Safer Health System (National Academies Press, 2000). doi:10.17226/9728.
5. International Organization for Standardization. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements (2022). <https://www.iso.org/standard/27001>. Accessed 18 Jul 2026.
6. OWASP Agentic Security Initiative. Agentic AI – Threats and Mitigations. OWASP (2025). <https://genai.owasp.org/resource/agentic-ai-threats-and-mitigations/>. Accessed 30 Jun 2026.
7. Goddard, K., Roudsari, A. & Wyatt, J. C. Automation bias: a systematic review of frequency, effect mediators, and mitigators. *J. Am. Med. Inform. Assoc.* 19, 121–127 (2012). doi:10.1136/amiajnl-2011-000089.
8. Lyell, D. & Coiera, E. Automation bias and verification complexity: a systematic review. *J. Am. Med. Inform. Assoc.* 24, 423–431 (2017). doi:10.1093/jamia/ocw105.
9. Agency for Healthcare Research and Quality. About Learning Health Systems (2019). <https://www.ahrq.gov/learning-health-systems/about.html>. Accessed 30 Jun 2026.
10. Carayon, P. et al. Work system design for patient safety: the SEIPS model. *Qual. Saf. Health Care* 15 Suppl. 1, i50–i58 (2006). doi:10.1136/qshc.2005.015842.
11. Holden, R. J. & Carayon, P. SEIPS 101 and seven simple SEIPS tools. *BMJ Qual. Saf.* 30, 901–910 (2021). doi:10.1136/bmjqs-2020-012538.
12. Clegg, C. W. Sociotechnical principles for system design. *Appl. Ergon.* 31, 463–477 (2000). doi:10.1016/S0003-6870(00)00009-0.
13. Wong, A. et al. External validation of a widely implemented proprietary sepsis prediction model in hospitalized patients. *JAMA Intern. Med.* 181, 1065–1070 (2021). doi:10.1001/jamainternmed.2021.2626.
14. Finlayson, S. G. et al. The clinician and dataset shift in artificial intelligence. *N. Engl. J. Med.* 385, 283–286 (2021). doi:10.1056/NEJMc2104626.
15. Sculley, D. et al. Hidden technical debt in machine learning systems. *Adv. Neural Inf. Process. Syst.* 28, 2503–2511 (2015).
16. Amershi, S. et al. Software engineering for machine learning: a case study. *Proc. IEEE/ACM 41st Int. Conf. Softw. Eng. Softw. Eng. Pract.* 291–300 (2019). doi:10.1109/ICSE-SEIP.2019.00042.
17. Kreuzberger, D., Kuehl, N. & Hirschl, S. Machine learning operations (MLOps): overview, definition, and architecture. *IEEE Access* 11, 31866–31879 (2023). doi:10.1109/ACCESS.2023.3262138.
18. Mitchell, M. et al. Model cards for model reporting. *Proc. Conf. Fairness Accountability Transparency* 220–229 (2019). doi:10.1145/3287560.3287596.
19. Gebru, T. et al. Datasheets for datasets. *Commun. ACM* 64, 86–92 (2021). doi:10.1145/3458723.
20. Raji, I. D. et al. Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. *Proc. 2020 Conf. Fairness Accountability Transparency* 33–44 (2020). doi:10.1145/3351095.3372873.
21. Arnold, M. et al. FactSheets: increasing trust in AI services through supplier's declarations of conformity. *IBM J. Res. Dev.* 63, 6:1–6:13 (2019). doi:10.1147/JRD.2019.2942288.
22. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29 (2024). doi:10.6028/NIST.CSWP.29.
23. U.S. Department of Health and Human Services. Summary of the HIPAA Security Rule (2024). <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>. Accessed 30 Jun 2026.
24. Office of the National Coordinator for Health Information Technology. Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Final Rule (2024). <https://healthit.gov/regulations/hti-rules/hti-1-final-rule/>. Accessed 30 Jun 2026.
25. Centers for Medicare & Medicaid Services. 2024 CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F) (2024). <https://www.cms.gov/initiatives/burden-reduction/overview/interoperability/policies-regulations/cms-interoperability-prior-authorization-final-rule-cms-0057-f>. Accessed 30 Jun 2026.
26. U.S. Food and Drug Administration. Clinical Decision Support Software: Guidance for Industry and Food and Drug Administration Staff (2026). <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software>. Accessed 30 Jun 2026.
27. U.S. Food and Drug Administration. Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions (2025). <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence>. Accessed 30 Jun 2026.