

Capture the Operator Knowledge an AI Supplier Still Needs

A Utility and Industrial Management Method for Usable Context

Phil Hatch | Akholi

October 23, 2026

Operators should identify the local knowledge that an outsourced AI service needs to interpret assets, conditions, and exceptions correctly. Documentation should preserve authoritative meaning and qualified escalation rather than convert unexamined operator habits into agent instructions.

Identify Knowledge That Determines the Action

The operations manager should ask which local facts and judgments make the proposed supplier service usable. Asset names, historical faults, operating constraints, maintenance practices, and unusual conditions can be understood by experienced staff but absent from formal records.

Allied operational-technology guidance emphasizes integration with safety and existing operating controls.¹ It is voluntary guidance, not an engineering approval. The manager should involve qualified site and engineering owners to determine what knowledge the particular service requires.

¹ Cybersecurity and Infrastructure Security Agency and Australian Signals Directorate et al., “Principles for the Secure Integration of Artificial Intelligence in Operational Technology,” Cybersecurity and Infrastructure Security Agency and Australian Signals Directorate et al., December 4, 2025, secs. 2.4 and 4.2, “Embed Safety and Failsafe Mechanisms,” <https://www.cyber.gov.au/publication/principles-for-the-secure-integration-of-artificial-intelligence-in-operational-technology>.

For a hypothetical water-utility planning assistant, a nominally available pump may have a local restriction not reflected in the central asset file. The service should obtain the authoritative current condition or escalate uncertainty rather than infer operability from a clean record.

Separate Valid Local Context from Unsafe Workarounds

The study describes operational knowledge in personal notes and experienced personnel.² These banking accounts do not establish industrial safety conditions. They identify why the manager should test whether important context is held outside the records the supplier can access.

Not every informal practice should be encoded. Some reflect necessary expertise; others may be outdated, inconsistent, or contrary to approved controls. Capture the rationale, source, conditions, and owner, then have qualified people decide what becomes an authorized operating instruction.

Include the limits of the knowledge. A rule that works under one equipment state or environmental condition may be unsuitable elsewhere. The agent should not generalize a local example into unrestricted authority across sites, assets, or operating modes.

Use an Operator Knowledge Acceptance Record

Figure 1 proposes four links: consequential question, authoritative context, approved application, and field test. Record the responsible operator or engineer, evidence source, validity conditions, and route for resolving uncertainty. Preserve version and effective scope.

DOE's AI testbed work emphasizes evaluation under specified configurations and conditions.³ It does not certify the operator's deployment. The manager should test the actual supplier configuration against the local context and restrictions the engineering assessment identifies.

Use representative exceptions and ask experienced staff to explain why the expected action is appropriate. Then ask another qualified person to use the captured material. A completed interview is not evidence that knowledge has become usable or that the receiving team can recognize its limits.

² Phil Hatch, *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*, version 1.8.2 (Akholi, forthcoming manuscript dated November 1, 2026), Part 4, "Knowledge at Risk of Departure," <https://doi.org/10.2139/ssrn.7164559>.

³ US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *CESER Releases New Testbed to Advance LLM and Agentic AI Evaluation for Critical Infrastructure* (US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, July 16, 2026), configuration transfer and limit discovery, <https://www.energy.gov/ceser/articles/ceser-releases-new-testbed-advance-llm-and-agentic-ai-evaluation-critical>.

Figure 1. The operator knowledge acceptance record

Question	→ Authority	→ Application	→ Demonstration
Decision	Decision	Decision	Decision
Decision affected by local context	Qualified source and validity conditions	Bounded instruction and uncertainty route	Normal difficult and absent-expert cases
Evidence	Evidence	Evidence	Evidence
Why does this knowledge matter	Which interpretation is approved	How may the supplier use it	Can another qualified team apply it
Maintain one reconciled operating record across buyer and provider. Investigate gaps, assign corrective authority, and repeat the affected acceptance test.			

Author's proposed method; adapt to the service and applicable jurisdiction.

Source: Phil Hatch, proposed framework developed for this paper.

Maintain Context and Preserve Engineering Authority

Local conditions change through maintenance, asset replacement, operating experience, and revised rules. Assign ownership and review triggers. A provider should know which source is authoritative and when stale or contradictory information requires restriction or escalation.

EU, UK, Swiss, US, and other operators face different safety, environmental, professional, cyber, data, and continuity requirements. Qualified local specialists should determine applicable conclusions. A global knowledge template should support site-specific engineering authority rather than replace it.

The contract should define the supplier's permitted use, evidence access, updates, confidentiality, and transfer obligations. Capture enough context to support safe service operation while protecting sensitive infrastructure information. Technical access alone should not confer permission to change equipment or operating settings.

Accept Knowledge Through Demonstrated Use

A reasonable objection is that capturing tacit knowledge can never be complete. Prioritize decisions and exceptions whose misunderstanding could materially affect the service. State gaps and restrict unsupported actions. The objective is a defensible scope, not a claim that every operator judgment has been digitized.

Before production or expert departure, run normal and difficult cases through the captured knowledge and actual supplier workflow. Test uncertainty and escalation. Correct ambiguities, obtain qualified approval, and repeat affected cases before expanding authority.

The manager should accept the knowledge transfer when the service can use approved local context and recognize when it is insufficient. Valuable operator expertise should become an accountable capability, with its limits preserved, rather than an undocumented dependency or an unqualified set of instructions for an agent.

Evidence and Source Note

The study is a nonrepresentative cross-section of 850 vendor delivery-team respondents on 150 engagements serving Tier 1 financial institutions, collected during January–June 2026. Neither banks nor vendors corroborated the accounts. It establishes reported experience, not causation, legal breach, or market prevalence. Its application here is a mechanism to investigate, not an estimate of conditions in other industries. The author-supplied version 1.8.2 is dated November 1, 2026 and is cited as a forthcoming manuscript consulted October 23, 2026.⁴

This is an analytical decision paper based on the supplied study and selected primary public sources checked through October 23, 2026. The original contribution is an operator-knowledge acceptance record distinguishing authoritative local expertise from unvalidated workarounds and testing usable transfer. The proposed method has not been independently validated. Legal requirements depend on the entity, activity, jurisdiction, and effective provisions; supervisory observations, research, and professional commentary have distinct authority.

Bibliography

Cybersecurity and Infrastructure Security Agency and Australian Signals Directorate et al.. “Principles for the Secure Integration of Artificial Intelligence in Operational Technology.” Cybersecurity and Infrastructure Security Agency and Australian Signals Directorate et al.. December 4, 2025.
<https://www.cyber.gov.au/publication/principles-for-the-secure-integration-of-artificial-intelligence-in-operational-technology>.

Hatch, Phil. *Agentic AI Outsourcing at Tier 1 Financial Institutions: Full Study Report*. Version 1.8.2. Akholi. Forthcoming manuscript dated November 1, 2026. Author-supplied manuscript consulted October 23, 2026.
<https://doi.org/10.2139/ssrn.7164559>.

US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. *CESER Releases New Testbed to Advance LLM and Agentic AI Evaluation for Critical Infrastructure*. US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, July 16, 2026.
<https://www.energy.gov/ceser/articles/ceser-releases-new-testbed-advance-llm-and-agentic-ai-evaluation-critical>.

⁴ Hatch, *Agentic AI Outsourcing*, Introduction, “Executive Summary” and “Evidentiary Basis and Its Limits.”