



**Institute of
Commissioning &
Assurance**

FROM PROJECT COMPLETION TO OPERATIONAL CAPABILITY

Why Operational Readiness Has Become the
Strategic Capability That Determines Whether Assets
Actually Deliver Value^[1]

by David Tain. MSc. P.Eng
Institute of Commissioning and Assurance
Chairman of the Technical Committee |
VP Latin America & Mediterranean Region

The Illusion of Project Success

For decades, organizations have measured project success through the traditional “iron triangle” of cost, schedule, and scope. If a project is delivered on time, within budget, and according to specification, it is typically considered successful. Yet across asset-intensive industries such as energy, mining, infrastructure, manufacturing, and transportation, many technically successful projects continue to struggle once they transition into live operations. Delayed startups, unstable production ramp-ups, operational disruptions, safety incidents, and costly post-startup interventions remain common even after construction and commissioning have been completed successfully.

This recurring pattern reveals a fundamental issue: technical completion does not necessarily mean operational readiness. Organizations frequently assume that once an asset is mechanically complete and commissioned, the transition to operations will happen naturally. In reality, the most critical phase of the asset lifecycle often begins precisely when the project is declared complete. The challenge is no longer about building the asset: it is about enabling the organization to operate it safely, reliably, and sustainably under real operating conditions.

The transition from project delivery into operations introduces uncertainty, evolving system interactions, incomplete information, and rapid operational decision-making. Technical systems, operational teams, procedures, governance structures, and supply chains begin interacting simultaneously for the first time under live conditions. As a result, operational performance depends not only on equipment functionality, but on the organization’s ability to coordinate people, systems, risk management, and decision-making effectively.

Why Operational Transitions Become Unstable

Operational startups are fundamentally different from construction or commissioning phases because systems begin interacting dynamically under real operating conditions. During construction, systems are generally isolated and relatively controlled. During startup, however, technical assets, operators, digital systems, maintenance strategies, and organizational processes begin functioning together as a single socio-technical system.



All this creates a level of complexity that traditional project management methodologies are not fully designed to address. Small disturbances can propagate rapidly across interconnected systems creating a compound effect with significant consequences to the asset and the organization itself. A training gap, for example, may trigger operational errors, which then affect equipment performance, create production instability, increase operational pressure, and influence decision-making behaviors elsewhere in the organization. In complex operational environments, failures rarely emerge from isolated technical deficiencies; they emerge from interactions among technical, organizational, and human variables.

This explains why startups often become unstable even when systems have passed commissioning and testing activities successfully. Equipment that performs correctly in isolation may behave differently once exposed to live operational conditions, fluctuating production demands, human variability, and commercial pressures. The startup phase therefore becomes one of the most risk-intensive periods in the entire lifecycle of an asset.

Moving Beyond the “Checklist” Mindset

Historically, Operational Readiness has often been approached as a procedural exercise driven by checklists, documentation reviews, and administrative validations. Many organizations focus heavily on confirming that procedures exist, training records are complete, and systems have been handed over technically. While these activities remain important, they are insufficient for managing the adaptive nature of operational transitions.

The problem with a checklist-driven mindset is that it assumes operational transitions behave linearly and predictably. This becomes particularly insufficient and dangerous when bringing a project to life as every step can derive adaptive events characterized by uncertainty, evolving conditions, and rapid operational feedback loops. Organizations cannot rely solely on procedural compliance when systems are continuously interacting and changing in real time.

This is where Operational Readiness must evolve conceptually. Rather than being viewed as a project phase near completion, Operational Readiness should be understood as a Strategic Organizational Capability that enables organizations to coordinate technical systems, operational teams, governance structures, and risk

risk management processes dynamically during periods of transition and uncertainty. Operational Readiness is not about verifying completion; it is about enabling operational adaptation.

Operational Readiness as a Dynamic Capability

Recent research increasingly aligns Operational Readiness with the theory of Dynamic Capabilities developed within strategic management. Dynamic Capabilities describe an organization's ability to sense changes, seize opportunities, and transform internal systems in response to evolving environments.

This perspective is highly relevant to operational transitions because startups are dynamic and uncertain environments. Organizations must continuously identify operational risks, mobilize resources to address readiness gaps, and adapt operational processes rapidly as conditions evolve. Operational Readiness therefore functions as a dynamic capability that enables organizations to transition from project execution into sustainable operations while navigating uncertainty effectively.

The implications are significant. Operational Readiness should not be reduced to procedural verification activities supported by software tools. Instead, it should be treated as an organizational capability embedded into governance, risk management, leadership structures, operational planning, and decision-making processes. It becomes the mechanism through which organizations orchestrate adaptation during one of the most sensitive operational phases they will ever face. This also explains why many organizations continue struggling despite substantial investments in technology. Operational capability cannot simply be purchased through software implementation. It must be developed institutionally through governance structures, operational discipline, workforce preparedness, and integrated risk management.

The Three Orders of Operational Capability

To better conceptualize operational transitions, the paper introduces the “Three Orders of Operational Capability” framework. This framework proposes that

operational performance depends on three interconnected layers of organizational capability.

The first order of capabilities consists of Operational Execution capabilities. These are the routine operational functions that enable organizations to perform under stable conditions, including standard operating procedures, maintenance systems, equipment operation, workforce competence, and safety management systems. These capabilities are essential for day-to-day operations, but they are designed primarily for stability rather than transition.

The second layer is Operational Readiness capability itself. This capability focuses on preparing the organization to receive, start up, and operate a new asset effectively. It includes readiness assessments, workforce preparation, operational procedure development, maintenance integration, governance alignment, and startup planning. Operational Readiness serves as the bridge between project completion and operational execution by orchestrating systems, people, and operational processes into a coordinated operational framework.

The third and highest order corresponds to Outcome Assurance capability. While Operational Readiness focuses on enabling startup, Outcome Assurance focuses on sustaining reliable operational performance over time despite changing conditions and uncertainty. This capability relies on adaptive governance, continuous monitoring, operational learning, proactive response mechanisms, and organizational resilience. Outcome Assurance enables organizations not only to start operations successfully, but to sustain operational reliability continuously as systems evolve.

Figure 1 below depicts the conceptual model of the Three Orders of Capabilities framework.

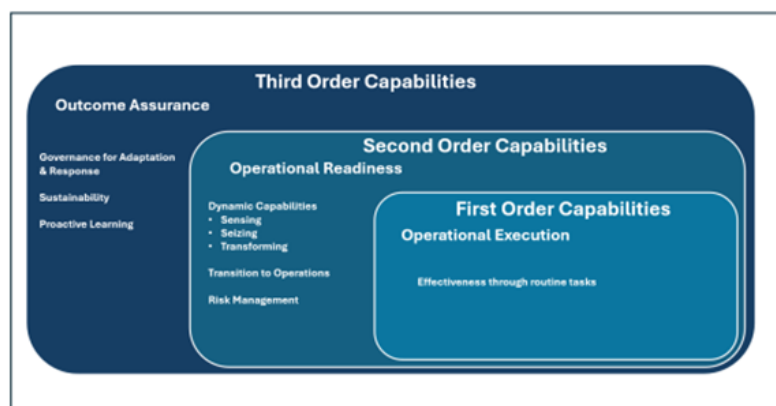


Fig 1: The Three Orders of Capabilities Framework

The insights in this framework allow to appreciate that operational performance is not created by isolated capabilities. Capability orders function as strategic layers that interact dynamically as part of a larger socio-technical system. Weaknesses in one layer rapidly propagate across others, amplifying operational instability.

Risk Management as Core Mechanism

One of the most important insights emerged from the Capabilities Framework is that risk management is not simply a supporting activity within Operational Readiness: it is its foundational mechanism.

Operational startups are inherently risk-intensive because systems begin operating under live conditions for the first time while organizations simultaneously face uncertainty, operational pressure, incomplete information, and evolving system behavior. Under these conditions, the organization's ability to identify, assess, prioritize, and respond to operational risks becomes critical.

Again, traditional project risk management approaches demonstrate often to be insufficient because they focus primarily on project execution variables such as cost and schedule impacts. Operational transitions require a broader and more integrated perspective on risk. Organizations must evaluate technical vulnerabilities, workforce preparedness, governance structures, interface management, operational procedures, maintenance systems, and human factors simultaneously.

This changes the role of risk management fundamentally. In the same fashion that adopting a checklist mindset is detrimental to Operational Readiness, risk management cannot be viewed merely as a compliance exercise or reporting mechanism. Risk management is the operational nervous system of the organization during transitional phases. It provides the mechanisms through which organizations identify emerging threats, prioritize operational vulnerabilities, allocate resources dynamically, and govern decisions under uncertainty.

This also explains why governance structures become so important during startup phases. Decision-makers must often act under incomplete information while balancing safety, operational performance, production objectives, and commercial pressures simultaneously.

Effective readiness organizations, therefore, establish structured governance mechanisms such as readiness reviews, escalation protocols, operational risk registers, and cross-functional coordination processes capable of responding dynamically as operational conditions evolve.

The Risk of Technology-Centered Thinking

As industries become increasingly digitized, organizations continue investing heavily in commissioning software, operational dashboards, predictive analytics platforms, and AI-powered monitoring systems. These technologies offer important advantages by improving visibility, automation, and data integration. However, technology alone cannot replace organizational capability.

One of the greatest risks organizations now face is the assumption that complex operational challenges can be solved primarily through digitalization. Software automates workflows and produces data, but it does not substitute for organizational judgment, governance, discipline, or risk-based decisions. Without strong governance structures and operational integration, digital solutions may indeed increase organizational vulnerability. Large volumes of operational data can overwhelm organizations and create a false sense of control while reducing their ability to distinguish meaningful operational threats from informational noise.

Technology should therefore be viewed as an enabler of Operational Readiness capabilities rather than a substitute for them. This is particularly important as, with the advancement of technology, the market sees an increased number of emerging digital solutions that, sold as expertise and sophisticated dashboards, are nothing more than data management systems that can't account for the unique variables an organization experience when bringing projects to life.

Digital tools can support monitoring and coordination, but it is the organization itself who must possess the capability to interpret signals, govern responses, and adapt operationally under uncertainty.

Lessons from Major Operational Failures

Several major operational failures illustrate these principles clearly in different industries.

A notable example of these failures in the Airport systems was the opening crisis of Heathrow Terminal 5. This case specifically demonstrated the consequences of confusing technical completion with operational preparedness. Although the terminal was completed successfully from an engineering standpoint, operational systems collapsed shortly after opening due to failures in baggage handling integration, workforce preparedness, and stakeholder coordination.

In the Power industry, on the other hand, the Texas Winter Storm Power Crisis exposed how infrastructure optimized for efficiency under normal conditions lacked the readiness and resilience required for extreme but foreseeable events. Failures propagated rapidly across interconnected energy systems because operational readiness and resilience mechanisms had not been institutionalized adequately.

A third example, the Deepwater Horizon oil spill in the Gulf of Mexico, showed the devastating consequences in the oil and gas industry of a failed readiness process. This case showed how weak governance structures, operational pressures, and inadequate risk-informed decision-making can transform technical anomalies into catastrophic failures.

In all three cases, the underlying issue was not simply technical deficiency. It was the absence of sufficiently mature organizational capabilities to manage operational complexity and uncertainty effectively.

The Strategic Capability That Will Define the Future

As industrial systems become increasingly interconnected, automated, and operationally complex, Operational Readiness will continue evolving from a technical support function into a strategic organizational capability. The organizations that consistently succeed in the future will likely not be those that simply deliver projects faster or cheaper, but those that are better prepared to transition assets into reliable, resilient, and sustainable operations.

All this calls for a fundamental shift in the execution mindset: Organizations must move beyond treating readiness as a procedural closeout activity and begin institutionalizing it as a capability embedded directly into operational governance, risk management, leadership, and decision-making structures.

Ultimately, projects do not generate value when they are completed. They generate value when they operate reliably, safely, and sustainably over time. In increasingly uncertain operational environments, the organizations that master Operational Readiness provides one of the most important competitive advantages of all: the capability to transform completed projects into stable and resilient operational systems capable of delivering long-term value.

Notes:

^[1] for full research paper, refer to: Tain, D. (2026) “Operational Readiness and Outcome Assurance: Capabilities for Adaptation, Risk Management and Decision-Making in Asset-Intensive Industries” *PM World Journal*, Vol. XV, Issue IV, 2026

URL: <https://pmworldjournal.com/wp-content/uploads/2026/04/pmwj163-Apr2026-Tain-Operational-Readiness-and-Outcome-Assurance-2.pdf>