KaufmanHall
a Vizient® company

March 2026

When systems go dark: why operational resiliency matters for treasury leaders

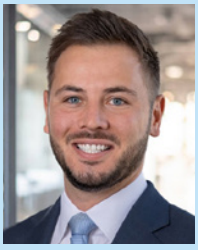
Introduction

At a time when clinical care, financial operations and patient experience increasingly depend on interconnected digital systems, operational resiliency within the finance function is not only a technical necessity, but it also ties directly to the patient care imperative. A prolonged network outage can disrupt everything from vendor payments and payroll to patient billing and revenue forecasting. Ensuring the system has access to sufficient liquidity during disruption can mean the difference between meeting obligations and failing to do so. The ability to maintain critical business functions during a digital disruption ensures continuity of care, protects organizational trust, meets regulatory obligations, and supports financial stability.

When all systems go dark

Imagine the day a health system confirms a network compromise, with destructive malware deployed deep inside the environment, and all systems go dark.

EHRs go offline for containment. Clinicians are unable to access records as identity systems are disabled. Patients cannot access their records. Financial systems, too, freeze. Enterprise Resource Planning (ERP) systems cannot authenticate users. Email and shared drives disappear. Claims stall. Payment workflows stop midstream. Cash visibility shrinks to whatever was printed or saved locally the day before.



Mike Signore
Vice President

This is no blip; no weekend system upgrade that teams can prepare for and muscle through. The system intentionally shuts down to prevent further spread. As paralysis intentionally sets in, the shutdown becomes the new operating environment for the next 30 days.

In that moment, providers no longer have just an IT concern. Some of the most critical questions become financial. Can the organization make payroll? What critical vendors need to be paid? Is there enough liquidity to withstand a month of disruption, all while keeping patient care as the top priority?

Downtime is often temporary. But a growing number of recent incidents in the industry have shown a different reality, one where cyberattacks expose financial and operational vulnerabilities as much as technical weakness. Proactively establishing operational resiliency becomes a finance leadership responsibility.

Operational resiliency, defined from the finance seat

From a finance perspective, operational resiliency is the ability to keep the most essential financial commitments intact during major disruptions to the systems, processes, or infrastructure that normally support financial operations. Rather than replicating business-as-usual in crisis conditions, it is about designing a "minimum viable finance function" that can operate under stress without compromising patient care, regulatory obligations, or the trust of staff and stakeholders.

During a realistic 30-day outage, the familiar infrastructure that ties everything together vanishes. And while IT is working to restore and harden systems, finance is operating in a very different world.

Arriving at clear priorities

Under these conditions, familiar questions become much harder to answer. Without usual integrations, payroll needs a way to build and transmit files. Accounts payable needs access to invoices and workflows that are unreachable. Borrowing, investing and responding to rating agency concerns becomes significantly more complex. These operational challenges come with real consequences. They rarely have satisfactory answers unless finance leaders work through them in advance.

Proactively establishing operational resiliency becomes a finance leadership responsibility.

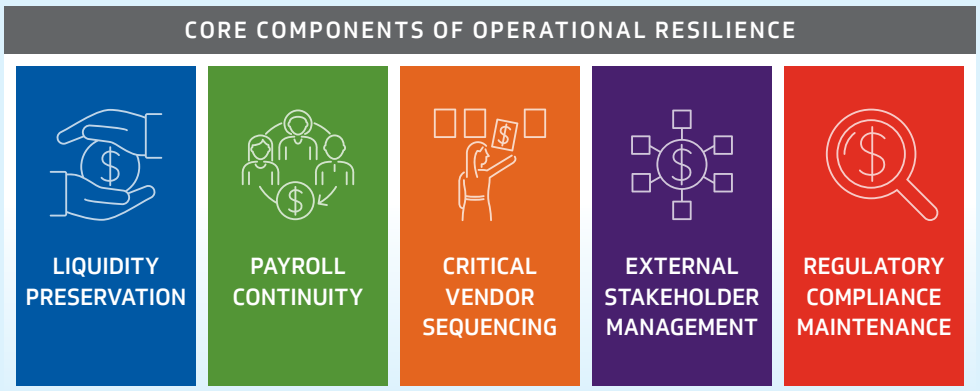
In a prolonged outage, supporting safe, continuous patient care becomes the primary objective, and achieving that requires clear priorities. Under genuine constraints, failing to prioritize because "everything is critical" is simply another way of choosing blindly.

Starting with the mission and working backwards quickly translates into a hierarchy of financial commitments: paying staff, ensuring key vendors are supported, meeting legal and regulatory requirements, and other needs as capacity allows.

Minimum viable finance function

The minimum viable finance function will vary depending on the organization.

The following five pillar framework establishes the core components of operational resilience:



Inventorying finance activities against this hierarchy clarifies what must continue and what can wait. Some processes, such as payroll and a subset of vendor payments, must continue on time, even if the method changes. Others, such as routine reconciliations or internal reporting, can be simplified or delayed without jeopardizing the organization. Still others can be paused, provided there is a clear plan to capture what happens during the outage and reconcile once systems return.

Once these priorities are understood, finance leaders can also quantify the organization's potential liquidity exposure before a disruption occurs, securing contingency funding proactively rather than improvising under duress. This means translating a potential outage into a cash model: expected daily cash inflows that could be delayed (revenue cycle and patient collections), fixed and mission-critical outflows that must continue (payroll, purchased services, debt service), and the timing/operational constraints on converting investments to cash. With those inputs, organizations can run scenario-based stress tests (e.g., 7/14/30-day outages) to measure risk, estimating peak cumulative cash need and defining triggers for actions like pre-negotiated line-of-credit capacity, collateral arrangements, minimum cash buffers, and revised liquidity policy thresholds. The outcome is a quantified "liquidity-at-risk" range that can be governance-approved and operationalized before systems go dark.

Making those distinctions explicitly, on paper, with alignment from executive leadership, creates a foundation for real resiliency. What deserves immediate attention and what can safely wait becomes clear and paves the critical path forward.

Designing continuity with control

Once priorities are clear, the next challenge is practical: executing critical activities when normal systems are unavailable.

For each essential process, finance leaders must define a workable path under outage conditions. The goal is adjusting operations for continuity with control. Accounts payable may not need to mirror the normal cadence. A curated list of truly critical vendors, paid on a reduced schedule through more manual processes, may be sufficient. Cash forecasting may shift from sophisticated models to a straightforward 30-day outlook built from bank balances and a handful of key inflows and outflows. When the unexpected occurs, teams can execute a deliberate plan rather than improvising under pressure.

Governance and communication when hard choices arise

Operational resiliency is as much about clarity and trust as it is about process and technology. Anticipating moments when not everything can be funded or completed on the usual timeline is an important aspect of resiliency planning. If those decisions are left to chance, the consequences can linger long after systems are restored.

Effective operational resiliency planning includes governance. Organizations should work to identify the individuals and

Principles for disruption preparedness

- Identify which external portals will remain accessible and secure with required credentials or tokens in advance
- Define the information required to execute critical processes and an alternate access source if core systems fail
- Establish segregation-of-duty protocols and documentation standards for offline execution
- Measure for and secure anticipated liquidity needs based on comprehensive risk analytics
- Maintain structured "downtime kits" with locally stored reports, templates, and contact lists
- Implement temporary manual controls such as dual signoffs or paper logs to preserve reasonable control for a limited period

teams with authority to re-sequence payments, draw on lines of credit, adjust investments, or deviate from normal policies, and under what conditions. These individuals can define thresholds for when the board or finance committee must be engaged, and how decisions will be documented when email and workflow tools are unavailable.

Equally, leaders and staff should know what to expect from the finance function during an outage: which services will be maintained, which will be limited, and how urgent issues can be communicated. Externally, transparent communication with banks, bondholders and key vendors can make the difference between a disruption that is understood and supported, versus one that erodes confidence and relationship capital.

From insight to action

Many organizations approach operational resiliency as an IT-led exercise. However, a finance-focused tabletop exercise of a simulated 30-day outage can expose gaps and surface practical fixes. The first exercise is often eye-opening. It is also not enough. The health systems that build true operational resilience treat this not as a one-time project, but as a discipline that sits alongside capital planning, liquidity management, and enterprise risk with a routine cadence.

To elevate operational resiliency from an abstract concern to a concrete management priority within the next 90 days, organizations can explore three next steps:

1. Assign an executive owner in finance for the "30-day offline" scenario, with a mandate to inventory critical functions and current gaps

Health systems that build true operational resilience treat it not as a one-time project but with a routine cadence.

2. Conduct a finance-focused drill that pressure-tests how payroll, vendor payments, liquidity management, and controllership would operate without core systems
3. Add operational resiliency on the agenda for the executive team or board risk committee, framed explicitly as a finance and patient-care issue, not just an IT topic

Organizations can continuously improve their foundation for resiliency: refining priorities, formalizing and documenting alternate workflows, and embedding outage scenarios into ongoing planning and stress testing. Finance leadership is uniquely positioned to drive that readiness. The question is no longer whether another disruption will occur. It is whether finance leadership has defined how the health system will protect solvency, sustain patient care, and govern decisively when systems fail. That requires clear decision rights, disciplined prioritization, minimum controls, and credible communication with banks, vendors, regulators, and the board. Operational resiliency is capital stewardship and fiduciary duty.

For more information, contact Mike Signore at michael.signore@kaufmanhall.com.