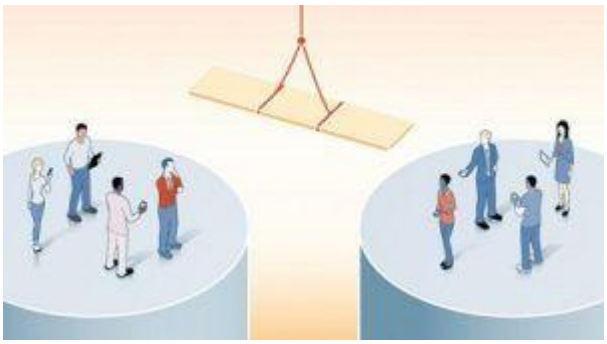
From Silos to Joint Operations: The Seismic Shifts Shaping the Future Operations Center

By Bruce McIndoe

February 1, 2026 | Security Today Magazine

"Operations centers have had a long season as "showcase environments"—impressive rooms with dashboards, screens, and steady streams of alerts. They demonstrate vigilance. They signal seriousness. But too often, they operate on the margins of the enterprise: monitoring the world, escalating issues, and proving compliance rather than delivering measurable advantages."

That model is becoming unsustainable.



The modern risk landscape does not arrive in neat categories. Disruption can begin as a cyber event and become a safety issue. A facilities failure can trigger business continuity decisions and reputational fallout. Geopolitical volatility can create travel risk, supply chain delay, and threat exposure to people and sites at the same time. Meanwhile, staffing constraints and alert overload are rising. Taken together, these converging pressures expose a stark truth: we cannot meet the moment, or the future, if we keep operating with physical security, cyber security, business continuity, crisis management, emergency management, and other protective disciplines as separate silos.

This reality calls for a new operational approach. A Future Operations Center is not about a larger video wall or more seats; it is about a fundamentally different way of working—multidisciplinary joint or combined operations, shared situational understanding, and an operating model that can quickly adapt to a changing environment. It also emphasizes integrated data, real-time analytics, and faster, more informed decision-making, shifting the focus from monitoring events to proactively shaping outcomes.

Words Matter: Stop "Converging" People—Start Unifying People to Missions

In many organizations, transformation efforts begin with language like "convergence" and "breaking down silos." But those phrases can unintentionally create resistance. People build careers by mastering discipline—earning certifications, developing hard-won judgment, building identity, and pride. Telling them they're going to be "converged" or "broken down" can land like an insult, not an invitation.

A better framing is "bridging the silos" and joint operations: different specialties maintaining their identity while working toward a common mission, anchored in shared data and shared outcomes. The goal isn't to erase tribes; it's to connect them.

That shift in language isn't cosmetic. It's operational. Because when an incident hits, success rarely comes from a single function operating alone. Success comes from the connective tissue between functions: the relationships, the handoffs, the shared playbooks, and the ability to coordinate quickly under pressure.

The Executive Disconnect: "Operational Resilience" Is a Priority—But the Organization Often Isn't Built for It

A recurring pattern in boardrooms and executive meetings is that leaders recognize operational resilience matters, yet their organizations are not structured to deliver it. Research from The Conference Board has found that most companies see disruption risk increasing and view operational resilience as a strategic priority, yet responsibility for operational resilience often sits several levels below the CEO, which can limit enterprise alignment and investment focus.

This is more than an org chart problem. It becomes an execution problem when critical capabilities are scattered across functions with different leaders, different budgets, different tooling, and different definitions of "success." In practice, the enterprise ends up with multiple "operations centers" that are excellent in their own lane, but poorly connected to one another.

If senior leadership expects resilience outcomes, they need a model that makes operational resilience more effective: integrated operations, consistent decision rights, and a shared foundation of trusted information.

The Real Measure of Resilience: Connections

One of the most practical predictors of resilience is not a policy binder. It's not the thickness of the plan. It's the number and strength of connections across teams.

When a disruption happens, most organizations do not pull a plan off the shelf and follow it line-by-line. Plans often "collect dust." What teams do pull, when they are effective, are recovery aids such as checklists and brief procedures. More importantly, they pull people together: facilities, HR, security, cyber, communications, safety, business owners, and outside partners. The organization can win (or lose) based on whether those relationships and operating rhythms exist ahead of time.

This is why "joint operations" is the core design goal. A Future Operations Center should institutionalize cross-functional coordination as a daily habit, so it doesn't have to be invented during a crisis.

Your Proof Point Is COVID: You Already Did This (You Just Didn't Institutionalize It)

Here's the part that lands with executives: most companies have already proven that they can operate as a mission-focused and sustained team.

When an existential threat such as COVID hit in 2020, organizations stood up with multidisciplinary task forces, often distributed regionally, with decision-making and adaptation close to where facts were emerging. Crisis leadership provided oversight, while cross-functional teams solved tactical and operational problems: access controls, health protocols, workforce decisions, travel, supply continuity, communications, and site-level adaptations.

That model wasn't just effective; it was life-saving for organizations.

And it raises a simple strategic question: if the organization can mobilize in that way for a sustained crisis, why not operate that way, at the right scale, for the mission that defines survival and competitiveness every day?

The gap isn't capability. It's institutionalization: embedding the lessons, the rhythms, and the connective tissue into how the enterprise runs day-to-day.

The Team-of-Teams Model: Shared Consciousness + Empowered Execution

"Team-of-Teams" isn't a buzzword; it's a proven organizational response to complexity. The essence is straightforward:

- **Shared consciousness**: high transparency, shared data, and a common understanding of what matters.
- **Empowered execution**: pushing decisions closer to where information is freshest, rather than forcing everything up and down a hierarchy.

This model is widely associated with Gen. Stanley McChrystal's concept of linking teams through shared context and decentralized execution to gain speed and adaptability at scale.

For operations centers, this is not philosophical, it's practical. A Future Operations Center can't be a single monolithic team that "does everything." It needs to be a coordinated network of teams that can surge, reconfigure, and collaborate quickly across disciplines. Also, this coordinated network of teams does not need to be in one physical location or building.

A good test: when a complex incident happens, do teams act like separate stovepipes (escalating into confusion), or do they act like a connected organism (coordinating, adapting, and executing)?

A Simple Foundation: Four Asset Classes (Plus the Processes That "Make the Magic Happen")

One of the most effective ways to simplify executive alignment is to recognize that most organizations ultimately protect and enable four core asset classes:

1. **People**
2. **Facilities and sites**
3. **Information and data**
4. **Supply and logistics**

Executive alignment also safeguards the processes that connect these assets to organizational objectives—that connective tissue is what truly defines the organization.

If operational resilience is about keeping critical operations running and recovering quickly when disruptions occur, why should the teams responsible for these assets continue to operate in disconnected silos?

A Future Operations Center is where these assets and processes become visible in a unified way: not as a static inventory, but as a living model that supports decisions and adapts as needed.

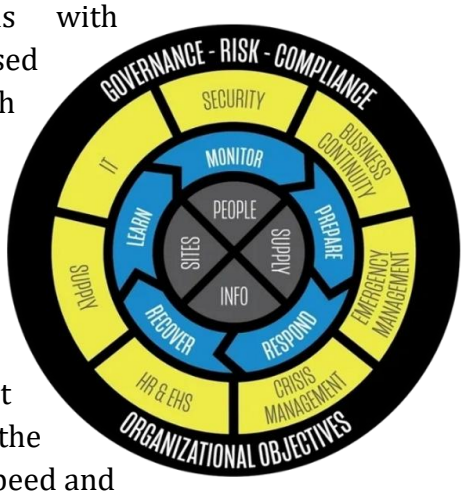
The Operating Loop: Continuous Risk Management, not "Spray and Pray"

Many organizations still operate a notification model that could be described as "spray and pray": blast notifications and alerts broadly and hope the right people act appropriately. But the next generation of operations demands a tighter, continuous loop. A Continuous Risk Management (CRM) loop:

1. **Monitor** (internal, perimeter, beyond-the-perimeter signals)
2. **Assess** relevance (Is this signal meaningful to our assets and objectives?)
3. **Determine impact** (What could this do to people, sites, information, supply, and operations? What would be the impact to the organization?)
4. **Notify and coordinate** (the right people, with role-relevant context and actions)
5. **Prepare or respond** (pre-position resources, mitigate, or execute playbooks)
6. **Recover and learn** (review, update procedures, strengthen relationships, enhance data)

JOINT OPERATIONS CONTINUOUS RISK MANAGEMENT MODEL

This CRM model aligns with established risk-based management concepts such as ISO 31000 Risk Management and Enterprise Security Risk Management (ESRM), which emphasizes linking activities to objectives and partnering with asset owners through risk methods.



The differentiator for the Future Operations Center is not the existence of this loop on paper, it's the ability to run the loop continuously, across multidisciplinary teams, with speed and precision.

Technology Is a Driver, But the Real Disruptor Is How It Changes Work

AI, automation, and virtualization are headline drivers, but their real impact is organizational: they change how decisions are made, how teams coordinate, and what "good" looks like in daily operations.

Soon, many enterprises will treat their data silos as raw material for connected intelligence ("unified knowledge layer"): domain-focused models or assistants for supply chain, people operations, facilities, risk, and security, interconnected to answer, "what does this mean for our organization?" with increasing specificity.

Done well, the organization can move from generic notifications and alerts to personalized, role-based insight:

- Which shipments, sites, or travelers are exposed?
- Which customers could be impacted, and by how much?
- Who must decide, who must act, and what options exist right now?
- What are the estimated operational and financial implications?

This is where virtualization and modern collaboration matter: the operations center becomes **less a place and more of a capability**—distributed, always-on, and able to coordinate across time zones and functions.

But this only works if the human system is ready: by using shared definitions, trusted data, clear decision rights, and practiced coordination.

What "Joint Operations" Looks Like in Practice

A Future Operations Center designed for joint operations tends to have several recurring characteristics:

1) A shared operating picture

Not a dashboard graveyard. A curated view of what matters: assets, dependencies, risk posturing, live incidents, and coordinated actions—accessible and tailored to the teams that need it.

2) Standardized playbooks and handoffs

Cross-domain procedures that clarify who leads, who supports, what thresholds trigger escalation, and how information flows.

3) Clear decision rights

A common failure mode is confusion about authority: cyber owns this, security owns that, facilities own that—until nobody owns the whole. A Team-of-Teams approach thrives when decision rights are explicit and practiced.

4) Operational rhythms

Brief daily or operating shift huddles for shared awareness, incident review cycles, and "command-of-teams" touchpoints during elevated risk. These rhythms are how shared consciousness is maintained.

5) Metrics that prove outcomes

A Future Operations Center earns executive sponsorship by measuring performance: time to detect, time to decide, time to coordinate, time to recover; reduction in duplicate effort; fewer handoff failures; improved readiness; and better business impact containment. Rather than just managing risk, we are measurably increasing the certainty that the organizational objectives can be achieved. Rather than talking about risk management to leadership, we need to be in the certainty management business that is measured through organizational outcomes.

Common Failure Modes to Avoid

As organizations modernize, a few traps recur:

- **Org chart "convergence" without joint operations:** moving boxes under one leader does not create shared understanding.
- **Tool sprawl:** adding more systems without an overall data governance model and a workflow backbone.
- **Undefined terms:** "incident," "event," "crisis," "emergency" used inconsistently, potentially leading to the wrong response at the wrong time. Words do matter.
- **Over-reliance on plans:** assuming documentation will substitute for practiced coordination. "Build capabilities, not plans."
- **Alert overload:** automation that produces more noise rather than clearly actionable information.

The antidote is disciplined integration: common language, standard data, coordinated processes, and a human system built for cross-functional execution.

What are the Key Benefits to an Organization – Both Internally and Externally?

Here are some of the key benefits of "Bridging the Silos"" and moving to a Team-of-Teams or similar operating model.

Benefits Internally to the Organization.

Organizational Benefits – "Bridging the Silos"

- **Enhanced Decision-Making** – Comprehensive visibility across all organizational functions
- **Resource Optimization** – Elimination of redundant systems, processes, and capabilities
- **Accelerated Innovation** – Diverse perspectives and knowledge drive breakthrough solutions
- **Operational Efficiency** – Streamlined workflows and faster communication
- **Improved Customer Experience** – Consistent delivery and reduced friction points
- **Organizational Agility** – Quick response to market changes and opportunities
- **Higher People Engagement** – Clear understanding of contribution to organizational success

Benefits Working with External Partners

External Partner Benefits Too

- Simplified Communications: Unified communication channels
- Timely Access to Information: Streamlined information sharing
- Fewer Interfaces: Enhanced coordination capabilities
- Streamlined Processes: Faster incident resolution
- Unified Approach: Better preparedness and planning
- Fewer Process and Handoff Issues: Consistent internal coordination
- Ease of Tracking Actions: Reduced response complexity
- Increased Transparency and Confidence: Improved compliance and regulatory relationships

A Practical Starting Point: 30/60/90 Days

For leaders building toward a Future Operations Center, a pragmatic path often looks like:

30 days: Map the reality

- Inventory existing operations centers and monitoring nodes (systems, processes, and data).
- Clearly define the shared vision and mission to align each team to.
- Identify the most common points of confusion or delay.
- Create a cross-functional leadership forum.

60 days: Pilot joint operations

- Train teams to work cross-functionally.
- Implement information sharing and transparency.
- Choose one cross-domain scenario (e.g., cyber + physical + continuity).
- Stand up a shared operating picture for that scenario.
- Run a tabletop *and* an operational drill focused on handoffs and decision rights.

90 days: Institutionalize the rhythm

- Shift from hierarchy to decentralized execution.
- Establish a standing cross-functional cadence.
- Define core metrics and measure them.
- Build a lightweight "unified knowledge fabric" connecting plans, procedures, and lessons learned to operational execution.
- Align technology and processes.
- Continuously evaluate and improve.

A Future Operations Center Is a Leadership Choice

It's tempting to treat a Future Operations Center as a technology project. But technology is only one driver. The deeper shift is cultural and operational: moving from separate siloed disciplines to joint operations, from siloed monitoring to shared sensemaking, from "spray and pray" messaging to coordinated decisions with measurable outcomes.

Organizations that succeed will not be the ones with the most screens. They will be the ones with the greatest number and strength of cross-functional relationships. This is manifested by multidisciplinary teams operating with shared consciousness and empowered execution, built into the way the organization pursues the achievement of its objectives every day.

That is the seismic shift: the operations center evolving from a place that watches, to a capability that delivers not just by managing risk, but by proactively increasing the certainty that the organization's objectives will be achieved every hour of every day.

About the Author

Bruce McIndoe is a global authority on risk management and organizational resilience and the founder of iJET International (now Crisis24). He currently leads McIndoe Risk Advisory, helping enterprises navigate complex and evolving security challenges.

Contact McIndoe Risk Advisory:

Web: www.mcindoeriskadvisory.com
Email: info@mcindoeriskadvisory.com
LinkedIn: www.linkedin.com/in/mcindoe