

The Dependency Blind Spot: Why Your Plan Stops at the Gate.

Assessing risks that live outside your facility walls—and how to measure them.

Corporate Taboos Series · Part 50 · Supply Chain · Risk Management · Resilience · Operations

The newsletter for VPs of Supply Chain who prefer honest diagnosis over comfortable denial.



The Missing Scope: Where Risk Really Lives

Most of us are excellent at managing what we can see. If a machine on your floor is throwing an error code, you have a process for it. If a batch of raw material arrives with the wrong dimensions, you have a non-conformance report and a path to resolution. We spend our days perfecting these internal controls—and they are vital. But there is a significant difference between managing your *operations* and managing your *dependencies*.

The problem is that many risk management plans stop at the fence of your facility. They focus on what you control, but they ignore what you need to survive. When we look at where risks actually live, the math tells a sobering story: roughly 43% of risk resides within your own walls (process errors, machine failures, and human mistakes). About 7% sits with your direct Tier-1 suppliers. But there is a massive gap—a "missing scope"—where less than 2% of our visibility meets the reality of the supply chain's deeper layers.

This isn't just about missing parts; it's about failing to see the connections between those parts and the infrastructure that makes them possible. If your plan only covers what is inside your gate, you aren't managing a resilient system; you are merely managing a local bubble. You might have a perfect control plan for your assembly line, but if that line requires a specific chemical from a supplier who relies on one specialized refinery three states away, your "perfect" plan has a massive hole in it.

The Dependency Blind Spot

I call this **The Dependency Blind Spot**. It is the failure to recognize that your production isn't just a series of independent steps; it is an interconnected web of dependencies that often stretch far beyond your immediate visibility.

Most companies approach risk with a linear mindset: *If I have a contract with Supplier A, and Supplier A says they are capable, then my supply chain is secure.* This is not "risk management." It is optimistic thinking. The reality is that Supplier A might be using a sub-component from Supplier B, who relies on a specific specialized tool owned by only one other company in the region.

When you rely on this linear logic, you create a single point of failure that stays hidden until it breaks. You aren't just risking a part; you are risking the entire flow because you didn't map the web—you only looked at the line. We must move from seeing "suppliers" to seeing "networks." If your risk assessment doesn't account for the fact that multiple of your Tier-1 suppliers might be sourcing their primary components from the same single source, you are operating with a blind spot as large as your warehouse floor.

Why We Live in the Walls

Why do so many organizations fall into this trap? It isn't because they aren't trying; it's often due to two very human factors: fear and complexity.

It is easy to manage what you can touch. You can walk onto the floor, see a broken fixture, and fix it. It feels like progress. Mapping out the entire infrastructure of your sub-suppliers' suppliers feels overwhelming and abstract. Many managers choose the "comfortable" path—focusing on their own internal metrics because they feel competent there—while ignoring the "harder" territory outside their direct control.

The Comfortable Rationalization	The Underlying Reality
"We can't manage what we don't control."	You cannot ignore a risk just because it is hard to map; if it impacts your ability to ship, you must account for it.
"Our Tier-1 supplier has handled this for years."	Their capacity is based on their own dependencies, which may be failing without their knowledge.
"It's too complex to track every sub-component."	It is better to know your three highest-risk nodes than to ignore them and hope they don't fail simultaneously.

We often mistake the lack of immediate complexity for a lack of risk. Because it's harder to see the problem, we tell ourselves that the problem doesn't exist until it hits our loading dock. That is not an operational choice; it's a strategic failure.

The Cost of Not Knowing What's Next

When you operate within your own "gate," the cost of ignorance only becomes apparent when things go wrong—and they usually fail in spectacular ways. This isn't just about a missing part from a shipment that is two days late. That's an operational hiccup.

The real cost is **Cascaded Failure**. When you don't know who your suppliers are buying from, or what infrastructure they rely on, you cannot prepare for systemic shutdowns. If a specialized high-heat furnace used by three of your Tier-s providers fails, and there is no alternative in the region, your production doesn't just slow down—it stops entirely.

The costs here are:

1. **Loss of Agility:** You can't pivot because you don't know where to look for alternatives until it's too late.
2. **Delayed Recovery:** When a failure occurs, your team spends days trying to figure out *why* it happened instead of fixing the problem.
3. **Reputational Erosion:** You have to tell your customers that you "don't know" when things will be back online because the root cause is buried three layers deep in someone else's basement.

A failure at a sub-tier level isn't just their problem; it becomes your production stoppage, your missed shipping dates, and your damaged reputation with your own customers.

Building a Resilience Operating System

To move past the gate, you need more than a better contract; you need an operating system for resilience. You must treat "dependency mapping" as a core part of your quality management system, not just something procurement does once a year during a contract renewal.

Here is how we structure that:

1. **Tier N Mapping:** You must identify the critical components in your build and map them back to their source at every level. If you don't know who provides the raw material for your Tier-1 supplier, you are flying blind.
2. **Concentration Analysis:** Identify where different suppliers share the same "bottleneck" resources—be it a specific port, a specialized chemical, or a unique piece of heavy machinery.
3. **Infrastructure Stress Testing:** Ask the hard questions about your partners' capabilities. Do they have enough safety stock? Do they have an alternative source for their primary components? If you don't know the answer to these, your "security" is just an assumption.

4. **Redundancy Validation:** A secondary supplier isn't a backup unless it's already qualified and capable of handling volume. You need to verify that the alternate path actually works before the primary one fails.

Operationalizing the 'Beyond' View

Knowing you have a problem is only half the battle; you have to know what to do on Monday morning. To get this off the ground, you must assign clear ownership and set a cadence for review.

Who owns it? This shouldn't just sit with procurement. It requires a partnership between procurement (who manages the relationship) and quality/engineering (who understands the technical requirements of the part). You need someone who can look at a component and say, "If this specific sub-component fails, our line stops."

The Action Plan:

1. **Identify the Top 10:** Start with your top ten most critical components—the ones that would shut down the plant if they disappeared for a week. Map these to Tier 3. This is your "High Risk" list.
2. **Audit Frequency:** Don't let these maps sit in a folder. Review them quarterly. Supply chains are dynamic; new trade routes, geopolitical shifts, and manufacturing changes happen constantly.
3. **The "What If" Drill:** Once a quarter, pick one high-risk dependency from your map and run a tabletop exercise. If this specific sub-component became unavailable today, what is our move? Do we have an alternate source? Can we re-engineer the part?

Stop looking only at your own machines and your own floor. The risks that can truly cripple your operation are often sitting just outside your gate. It's time to map the territory beyond the fence.

Call to Action

Where does your current risk assessment stop? Share this with another leader who needs to look beyond their own factory walls.

Newsletter replies: newsletter@sixsigmakaizen.com · X: [@kaizen_6sigma](https://twitter.com/kaizen_6sigma)

Stay curious, stay improving,

David Rodgers

SixSigmaKaizen.com

References: Study: Supply chain disruption may come from beyond a company's own walls