Global Software Delivery in a Fragmented World

How can multinational organizations design resilient delivery models as the globalized model begins to show cracks?

THE NEW PRESSURE POINTS

Geopolitics

AI Acceleration

Timezone Frictions

Executive Summary

Thinking Globally, Operating Under Local Constraints

For nearly three decades, multinational companies organized software delivery according to the logic of globalization. Professionals, software, hardware, data, and intellectual property (IP) moved across borders with relatively few constraints. That model is now under pressure.

Now, three forces are restructuring global software delivery models for multinational organizations. The first is geopolitical fragmentation. Governments increasingly treat technology infrastructure, data, and IP as strategic assets tied to national interests.

The second force is AI-driven acceleration. Generative AI speeds up parts of the development cycle, particularly coding and documentation, but shifts friction to other parts of the process, such as architecture design, system integration, and code review.

The third force is coordination friction across time zones. As development cycles become shorter, delays between distributed teams become more costly. The time you gain with AI can be quickly erased when teams can't work in sync. When one team logs off as another logs in, simple decisions take hours, sometimes a full day.

Together, these forces are pushing CIOs and technology leaders to reconsider several aspects of their delivery models. They must evaluate where vendors are located, how geopolitically aligned their partners are, where teams are distributed, where data is stored, and whether critical capabilities should move closer to home.

THE CORE CHALLENGE IS RESILIENCE.
IN A MORE FRAGMENTED WORLD, DISRUPTIONS AFFECTING A REGION, VENDOR, OR INFRASTRUCTURE LAYER CAN SLOW OR INTERRUPT DELIVERY PIPELINES.

1. The New Pressure Points in Global Software Delivery

1.1 / Geopolitics and the Strategic Value of Technology

If the global economy had a weather forecast, 2026 would read: **stormy.**

According to the World Economic Forum's Global Risks Report 2026, geoeconomic confrontation ranks among the most significant near-term risks for global businesses. Roughly half of the leaders surveyed expect the international outlook to remain *"turbulent"* over the next two years. Other concerns highlighted by the executives include armed conflict, misinformation, and cyber insecurity.

Global operations are getting harder to manage. Political decisions, regulatory shifts, and regional tensions now shape how multinational companies choose partners, structure teams, and design delivery pipelines. Governments are stepping in too, treating software, data, and IP as strategic assets tied to technological leadership and national security.

As a result, national administrations are paying closer attention to how these assets move across borders. This growing scrutiny is already changing the relationship between companies and their technology vendors.

Key Stats:

60%

of leaders say geopolitical tensions already influence their cybersecurity strategy.

Source: WEF

9%

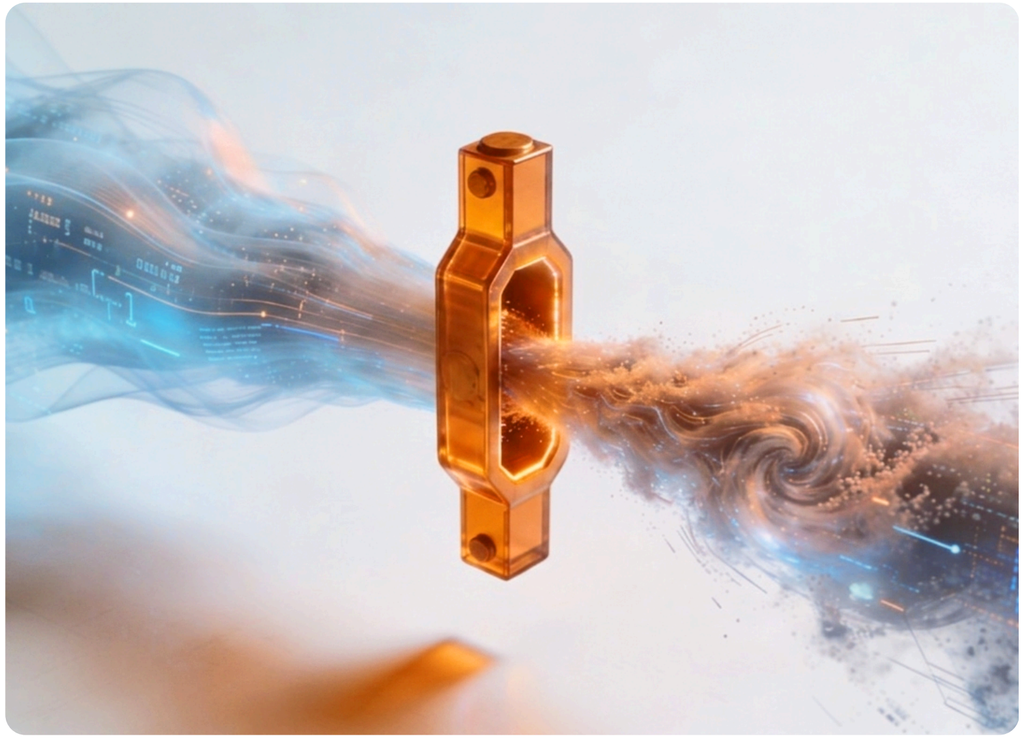
of respondents expect global stability in the near term.

Source: WEF

For years, vendors delivered services across jurisdictions under relatively predictable conditions. Clients expected safeguards to protect sensitive data and IP, but those requirements were largely framed around contractual compliance and corporate risk.

Today, the bar is significantly higher. Organizations now examine vendors not only for technical capability and cost efficiency, but also for their ability to operate under stricter security requirements and data governance standards.

These changes carry strategic implications for multinational companies. Many organizations built their software delivery pipelines assuming a relatively frictionless world where they could move any of those resources across borders with limited constraints. In a more fragmented geopolitical context, that model is beginning to show signs of exhaustion.



1.2 / AI Acceleration and the Changing Development Pipeline

Much of the current discussion around software delivery focuses on how AI tools are transforming the development process. As widely recognized across the industry, generative AI has accelerated parts of the software development cycle, particularly code generation.

However, it has not replaced the experience, judgment, or architectural responsibility of software engineers. Instead, what we are seeing is a redistribution of friction across the development pipeline.

The bottleneck is no longer concentrated in writing code itself. It now appears in other parts of the DevOps chain: reviewing AI-generated code, integrating it with existing systems, defining architecture, and deciding how different components should interact within complex environments.

Bain & Company estimates that productivity gains in software development can range between 10 and 15 percent when AI tools are integrated into the workflow. But those gains interact with another structural constraint that multinational organizations have long faced: coordination across distributed teams operating in distant time zones.

A simple example shows the issue. A developer moves forward with a feature until they hit a dependency on an API interface. They need clarification from another team before continuing. They send a message on Slack, but the other team is offline.

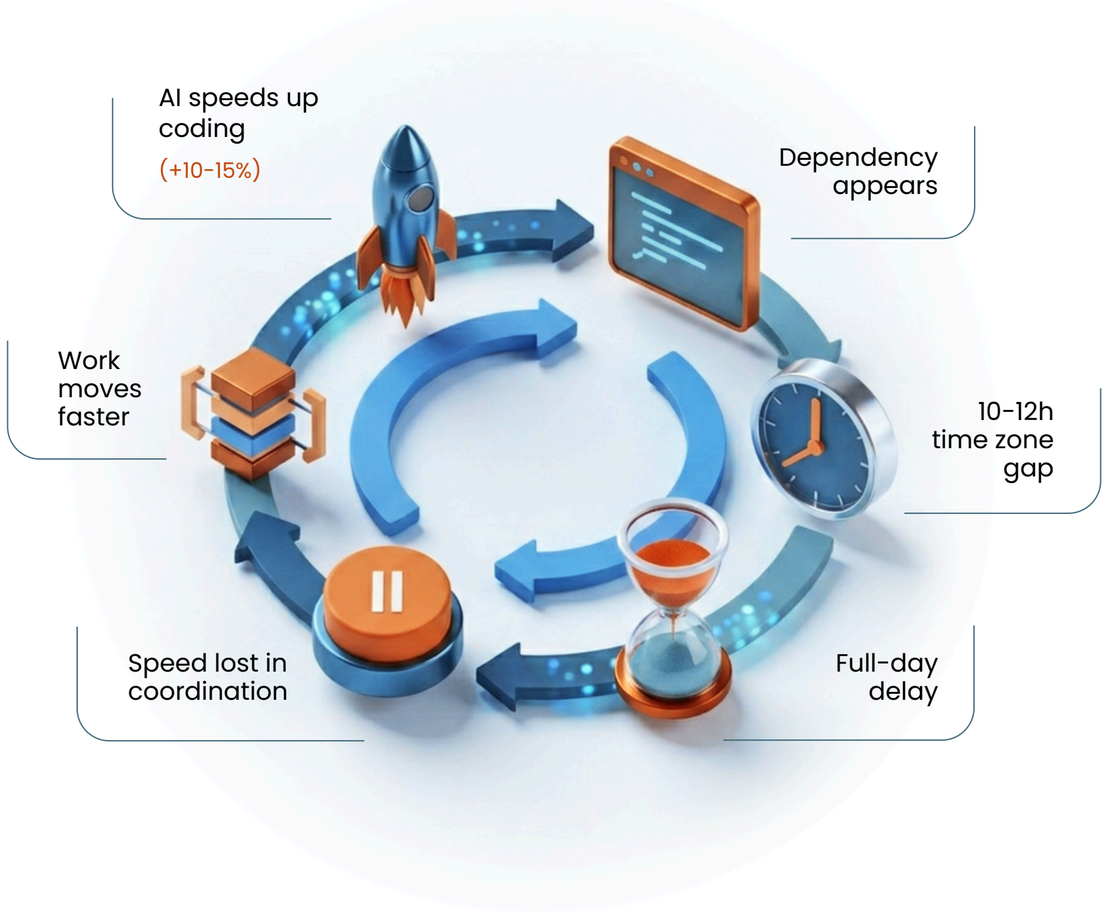
When teams operate with time differences of ten hours or more, even small questions can take an entire day to resolve. What could have been addressed in a short conversation becomes a full cycle of asynchronous communication.

This is not a question of individual productivity. It is a structural characteristic of the delivery model. When development cycles were slower, teams could often absorb these coordination gaps. But as AI compresses parts of the development pipeline, those frictions become more visible and more costly.

The time saved through faster coding can quickly disappear when decisions, reviews, and integrations depend on asynchronous coordination.

Which raises an important question for multinational organizations:
If AI accelerates development, can globally distributed delivery models keep pace with that speed?

AI Speeds Up Coding...
But Where Does the Time Go?



2. Strategic Responses to a Fragmented World

In this context, McKinsey identifies two broad strategic responses. At the same time, our experience working with Fortune 500 organizations operating globally suggests that a third approach is also beginning to emerge.

Some organizations continue to operate under unified global delivery models but add stronger safeguards around governance, vendor diversification, and geopolitical exposure. Others introduce structural segmentation to reduce regulatory and geopolitical risk.

A third model is gradually taking shape. It keeps strategically sensitive assets closer to home while maintaining distributed delivery capacity across trusted regions. We refer to this approach as selective localization with deliberate distribution.

This reality also changes how companies evaluate technology partners. Organizations now scrutinize vendors and outsourcing providers more closely, examining certifications, governance standards, and their ability to work under stricter regulatory and security requirements.

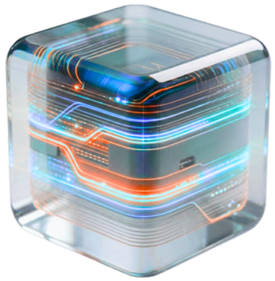
Many companies are also revising the geography of delivery. Some expand nearshore models to maintain access to global talent while working within overlapping time zones.

Others strengthen onshore capacity, accepting higher costs in exchange for tighter control over critical systems and data.

Hybrid approaches are also gaining traction. Models such as smartshore delivery combine local delivery centers with nearshore engineering teams, allowing organizations to balance resilience, time zone coordination, and access to specialized talent.

In short, the companies that will “win” in this fragmented world will be those that preserve the advantages of operating globally while following the rules of what many analysts describe as *“glocalization”*: thinking globally while complying with national/local rules.

2.1



One global delivery model

(non-naïve globality)

Some organizations are acting under a unified global model, but without assuming a frictionless world.

They maintain centralized platforms, shared governance, and global vendors, while adding stronger safeguards around risk exposure. This includes vendor diversification, stricter governance, and prioritizing partners in geopolitically aligned regions. This model preserves scale, consistency across regions, and agility.

However, it also maintains exposure to cross-border dependencies. Resilience depends on how well organizations manage vendor risk, regulatory shifts, and geopolitical uncertainty within a still interconnected structure.

SCALE & EFFICIENCY

2.2

Structural Segmentation

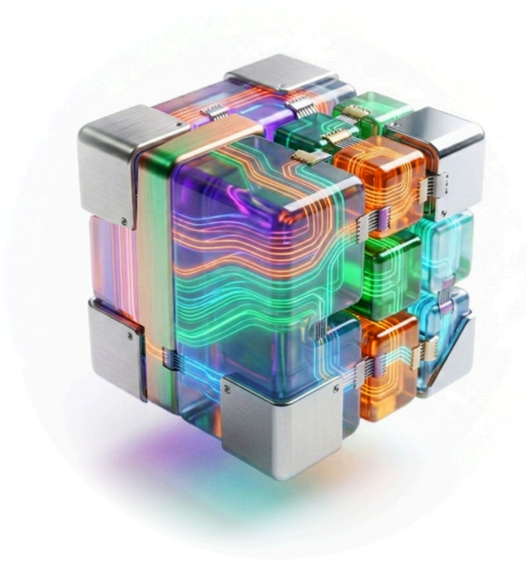
Other organizations redesign their delivery model by introducing regional separation.

They isolate systems, data, and teams to reduce regulatory and geopolitical risk. This approach limits cross-border dependencies and increases control over sensitive assets such as IP and regulated data.

It is common in highly regulated industries. Organizations adopting this model accept these costs in exchange for greater control and resilience.

CONTROL & ISOLATION

2.3



A third path is emerging:

Selective localization with deliberate distribution

Our experts are starting to see a third model emerging for multinational organizations trying to balance global scale with local control.

Instead of going all-in on centralization or fully splitting everything by region, companies are becoming more deliberate in how they organize delivery. They keep what really matters closer to home, or within regions they trust, and place the rest elsewhere, but under clearer rules.

Not everything carries the same level of risk. Core platforms, sensitive data, IP, AI models, and key architectural decisions need tighter control and closer alignment with local regulations.

That kind of work tends to stay onshore or within geopolitically aligned regions.

Other activities and resources, like development, testing, or engineering teams, can still be distributed across different locations. But not just anywhere.

Companies now look for teams that share similar time zones, so conversations don't drag across days. They keep roles like service management closer to the business, where decisions can happen quickly. And they prefer partners in regions that follow similar regulatory standards and geopolitical alignment.

What you get is a more balanced setup. Companies still tap into global talent and more convenient cost structures, but without leaving their most critical assets exposed.

PROTECT THE CORE. FLEX THE EXECUTION.

Expert Insight

“Not everything requires the same level of protection. ***What matters is knowing what’s critical and making sure those pieces are close, aligned, and easy to respond to.*** *Time zones play a big role there as well.”*

NICK BACA-STORNI
Managing Partner, Inclusion Cloud

3. When Intellectual Property Becomes a Strategic National Asset

As geopolitical tensions intensify, intellectual property is no longer treated solely as a corporate asset. It is increasingly tied to national competitiveness, technological leadership, and economic security.

This shift is changing how governments, regulators, and enterprises approach data, software, and research assets. What once moved relatively freely across borders is now subject to closer scrutiny.

For multinational organizations, this raises a new question: how to protect critical knowledge while still operating across distributed delivery models.

3.1 / Why IP Protection Changes the Delivery Model

Protecting sensitive and critical information stopped being a problem for the legal desk a long time ago.

As organizations became more digital, and now with AI in the mix, the number of parties involved in building and running the business has grown. Partners, vendors, freelancers, and platforms all interact with this data, creating an increasing number of windows for potential exposure.

This creates new constraints:

- **Limiting** access to critical systems and data
- **Restricting** where certain workloads can run
- **Reducing** exposure across vendor ecosystems

Key Stats:

1 in 3 CEOs

ranks cyber espionage and IP theft among top strategic risks.

Source: WEF

95%

of data breaches involve a human element.

Source: Splunk

3.2 / The Pharmaceutical Industry as a High-Stakes Example

To understand how these risks play out, it helps to look at pharmaceuticals, where IP is not only a key asset but the foundation of R&D investment. The promise of exclusivity is what allows companies to invest billions over years of research.

At the same time, these assets go beyond corporate value. As seen during COVID-19, drug formulas, vaccines, and manufacturing capabilities can quickly become matters of national interest, tied to public health and strategic autonomy.

There is another layer to this. Drug discovery now relies heavily on software, from molecular simulations to clinical data and regulatory systems. Protecting IP increasingly means protecting how these systems are built, accessed, and connected.

Those systems follow the same logic we explored earlier. They are developed by distributed teams, rely on external vendors and cloud platforms, and involve constant data flows across environments.

The challenge becomes sharper with AI in the loop. Models may generate responses influenced by training data that includes licensed or third-party research, raising questions about IP boundaries. At the same time, without proper guardrails, everyday interactions between scientists and AI systems can become a channel for unintended data leakage.

SAP Access Control as a Foundation for IP Protection

Platforms such as SAP Governance, Risk, and Compliance (GRC) and SAP Identity Access Governance (IAG) provide a foundational layer to protect sensitive pharmaceutical IP.

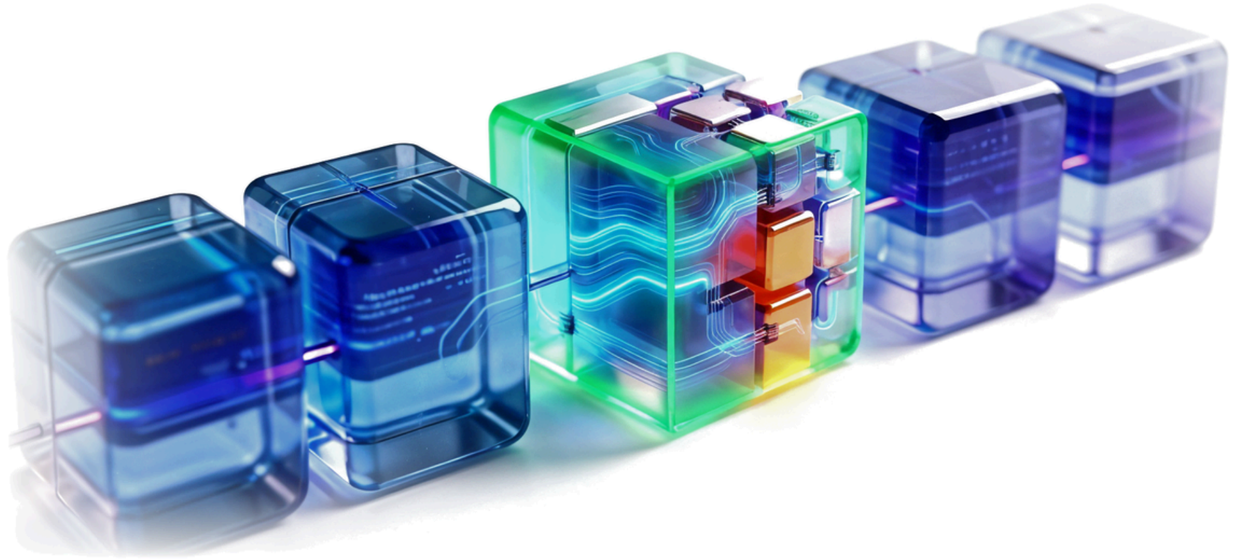
They help organizations define roles, enforce segregation of duties, and control who can access critical data across systems and external partners.

As SAP partners, we typically see this as a practical starting point for organizations looking to strengthen control over sensitive information, especially in distributed R&D environments.

4. What You Should Ask Before Choosing a Technology Partner

Technical proficiency is no longer enough. Technology vendors are part of the software delivery chain, with different levels of access to systems, data, and critical workflows. As a result, the level of scrutiny is increasing.

Companies now expect certifications, clear governance models, and real proof of how vendors operate (especially in multinational environments where sensitive data and key intangible assets are involved).



This is the new baseline:

In practice, this level of scrutiny tends to translate into a set of recurring questions:

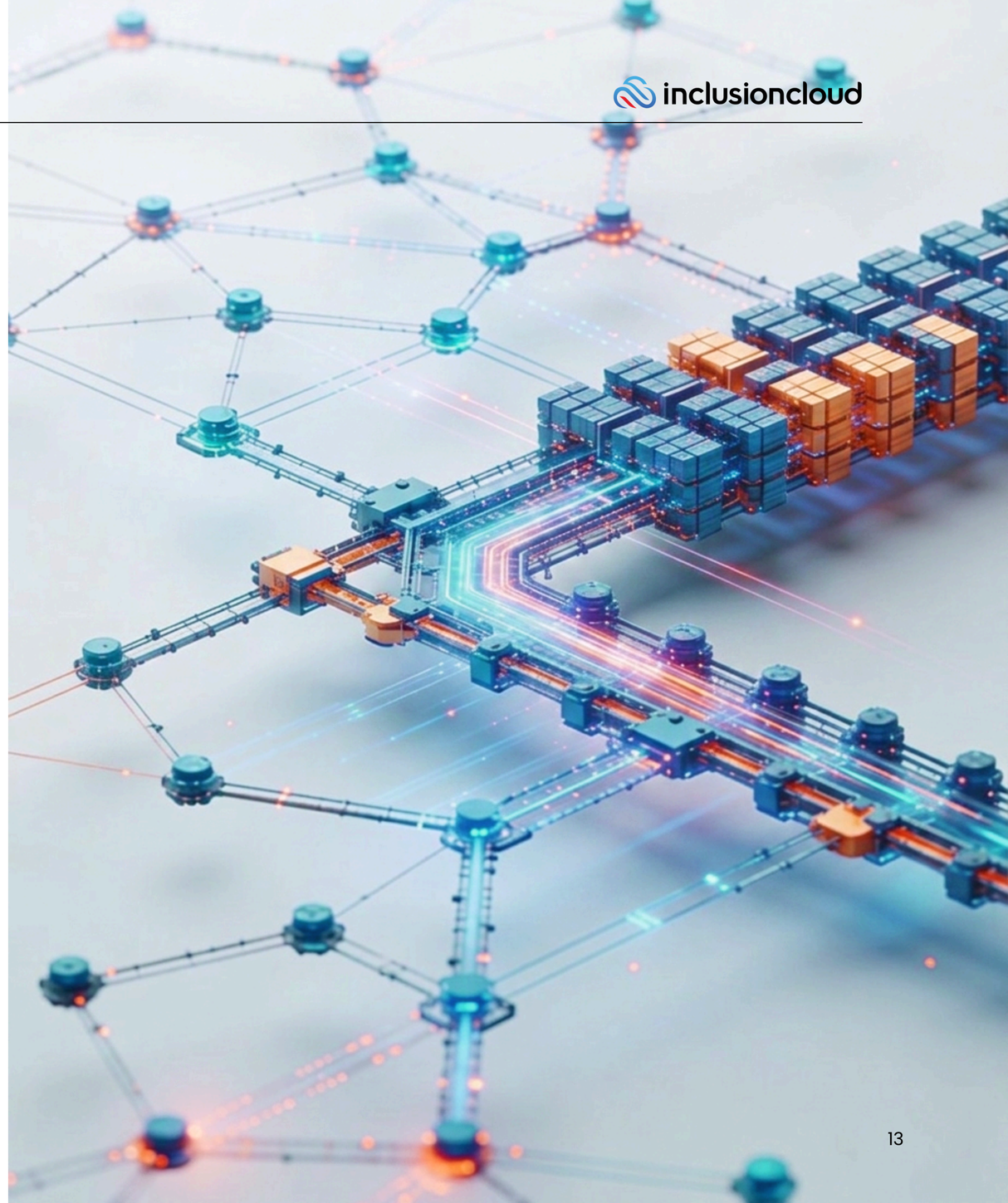
- Can your operations continue if regulations change or a region becomes unstable?
- What happens if a critical vendor or delivery team becomes unavailable?
- Where are your systems, data, vendors, and talent actually located—and under which jurisdictions?
- Where are the hidden concentration risks across regions or providers?
- How is sensitive data stored, accessed, and governed across environments?
- Who are your vendors?
- How are access rights, environments, and data flows controlled across regions?
- What role do AI tools play in delivery, and how is sensitive data protected in those interactions?
- How quickly can teams respond when conditions change?

5. More or Less Outsourcing?

In a context where operating across regions is becoming more complex, a natural question starts to surface: will companies outsource more, or less? At first glance, the global climate may suggest a pullback.

Stricter regulations, geopolitical tension, and tighter controls over data and vendors seem to point in that direction. However, the data suggests otherwise. The global outsourcing market is projected to reach $7.11 trillion by 2030 (Grand View Research), reinforcing the idea that outsourcing remains a structural component of how large organizations run.

From Nick Baca-Storni's perspective, this is less about volume and more about how delivery models adapt to current conditions. As geopolitical and regulatory pressure increases, companies don't evaluate outsourcing only based on cost. They also consider exposure: where vendors operate, under which jurisdictions, how those regions fit their risk profile, and how well these models perform in uncertain environments. In that context, time zone alignment plays a more central role. Traditional offshore models begin to show their limits under these conditions.



As Nick explains, offshoring works best in stable environments, where planning cycles are predictable and teams can absorb delays without major impact. That context has changed. Today, companies face stricter vendor requirements, place more weight on geopolitical alignment, and operate with shorter delivery cycles. When large time zone gaps enter the equation, coordination becomes harder to sustain. Teams working more than ten hours apart have limited overlap, which slows down communication, delays decisions, and increases the number of handoffs needed to move work forward.

"Offshoring is starting to show its limits because it works best when everything is stable. Today, vendor controls are much stricter. And when you add large time zone gaps on top of that, delivery risk increases very quickly."

This dynamic manifests in subtle but recurrent ways. When teams use asynchronous communication, even minor modifications might take a full day to resolve, as Nick experienced.

What appears to be a tiny delay right away accumulates over the delivery cycle, progressively undermining the efficiency benefits that AI and automation seek to achieve.

In volatile environments, where priorities shift quickly due to regulatory updates, security concerns, or sudden business decisions, this becomes more than an efficiency issue. It becomes a resilience problem. The longer it takes to respond, the longer organizations remain exposed.

Against this backdrop, the question is not whether outsourcing will increase or decrease, but how it will evolve to meet new constraints and comply with the growing requirements multinational companies face.

"I've seen cases where a small change takes a full day just because of time zone differences. Someone sends a message on Slack while they're online. The other team is asleep. When they reply, the first team is already offline again."

5.1 / Delivery models that fit this reality better

As organizations adjust to these constraints, they are increasingly prioritizing delivery models that allow for synchronous work, or at least meaningful overlap during most of the working day. The objective is not only to improve coordination, but to ensure that teams can respond quickly when conditions change.

Nearshore

Nearshore delivery is gaining traction because it allows teams to work in real time without losing access to broader talent pools.

When teams operate in similar time zones, coordination becomes easier, delays are reduced, and communication flows more naturally. This leads to a more consistent delivery rhythm, while still benefiting from more competitive and convenient cost structures.

Onshore

At the same time, onshore delivery is becoming more relevant for critical capabilities, especially in highly regulated industries or environments where sensitive data is involved.

Keeping these functions closer to the business centralizes control, making it easier to manage access and protect sensitive data.

Smartshore

Often referred to as smartshore, bestshore, or rightshore, these setups organize delivery based on what is critical and what can be scaled. Functions like architecture, governance, and service management stay close to the business, where control and fast response are key.

Execution capacity is then distributed across regions that enable real collaboration (typically those that share time zones or have strong operational alignment) so teams can work as one without introducing unnecessary friction.

From Nick’s perspective, what makes these models attractive is their adaptability. Flexibility becomes a way to manage risk.

6. Conclusion & Outlook

Global Scale, Local Rules

Software development has hit a turning point. AI is making the actual coding much faster, but that speed is exposing a major flaw: if your tools are fast but your communication is slow, you aren't actually gaining anything.

For a global enterprise, waiting overnight for a response from a team on the other side of the world used to be a manageable cost (justified by the bottom-line savings.). But today, because AI speeds up production, those time zone gaps have become massive roadblocks.

If you save five hours using AI but lose ten hours waiting for an answer from another region, you are moving backward. The old math of trading time for lower costs no longer adds up.

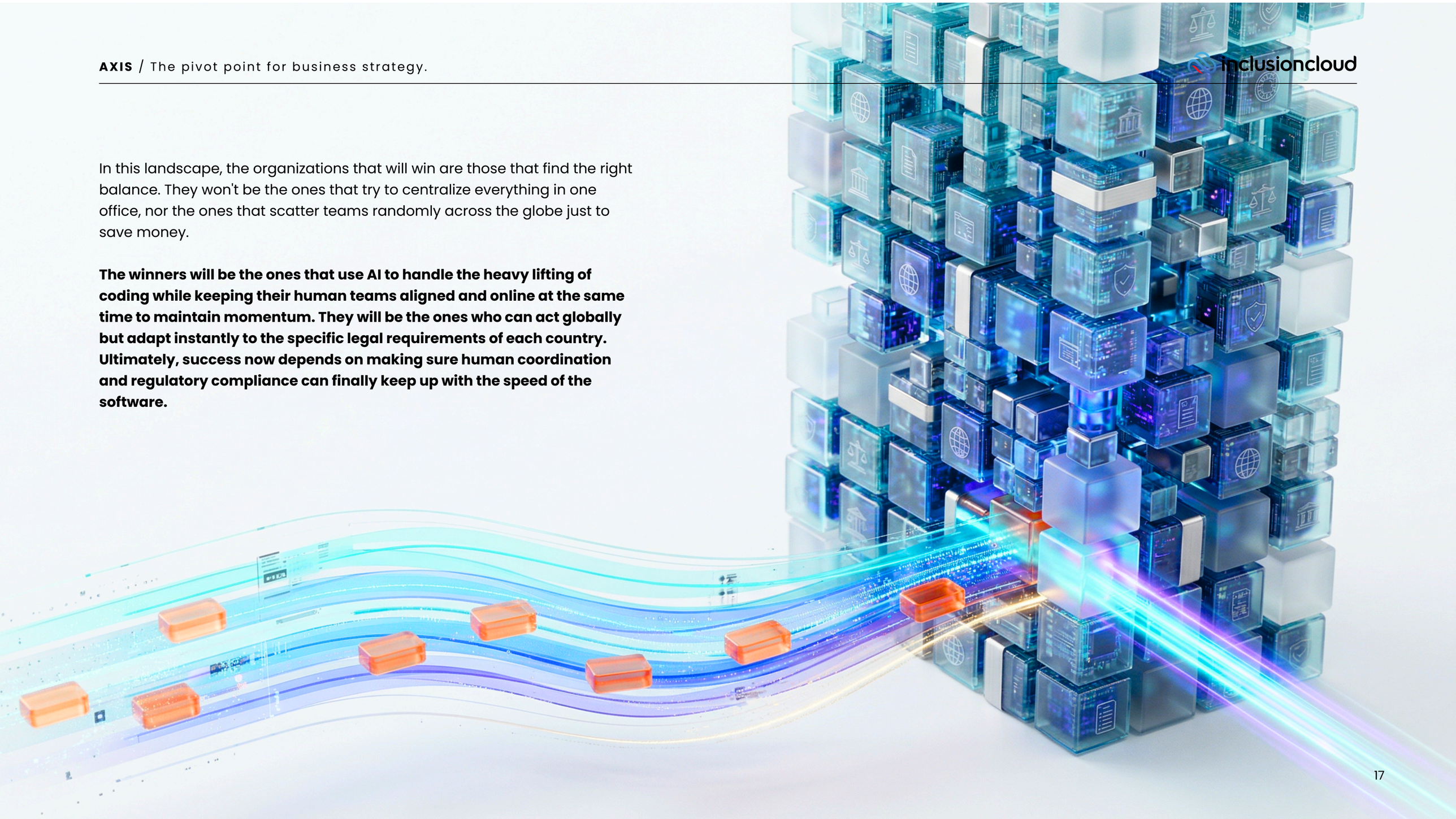
The challenge, however, isn't just about time; it's about the growing wall of local rules. We are moving toward a fragmented world where data protection, IP laws, and government regulations change depending on where you are standing. This is forcing multinationals to rethink their entire structure. Things are different now; you have to ensure that talent can operate within a complex web of enterprise governance and local mandates. Technical skill is now just the baseline. The real test is whether an organization can protect its data and stay compliant while operating at a massive scale in multiple different jurisdictions at once.

GLOBAL SCALE IS STILL THE GOAL.

LOCAL RULES ARE NOW PART OF THE REALITY.

In this landscape, the organizations that will win are those that find the right balance. They won't be the ones that try to centralize everything in one office, nor the ones that scatter teams randomly across the globe just to save money.

The winners will be the ones that use AI to handle the heavy lifting of coding while keeping their human teams aligned and online at the same time to maintain momentum. They will be the ones who can act globally but adapt instantly to the specific legal requirements of each country. Ultimately, success now depends on making sure human coordination and regulatory compliance can finally keep up with the speed of the software.



Disclaimer

The insights presented in this report draw from third-party research, industry publications, and Inclusion Cloud's own analysis of software global delivery pipelines and the IT outsourcing market. They reflect trends and perspectives observed across multiple sources, but they may not capture the full range of conditions across every industry or region.

While we aim for accuracy and relevance, readers should interpret these findings within the scope of the referenced material and the broader limits of market analysis. This report is intended for informational purposes only. It should not be considered financial, legal, or architectural advice. Inclusion Cloud is not responsible for decisions or outcomes resulting from the use or interpretation of this material.

About Us

Inclusion Cloud helps companies implement and optimize enterprise software, cloud solutions, data platforms, and AI capabilities. As certified partners of SAP, Oracle, ServiceNow, and Salesforce, we deliver the technical expertise and integrations that modern enterprises rely on.

Our AI-powered talent engine, inMOVE™ by Inclusion Cloud, combines advanced recruiting technology with rigorous technical validation to secure top certified resources. With more than 20 years supporting global organizations, we focus on building solutions that are scalable, integrated, and ready for the real world.

inclusioncloud

Discover how we're helping enterprises build what's next at inclusioncloud.com