THE kyndryl institute

Trend Topic: **Governance Risk and Compliance in the Age of AI**

By

Javier Olveira

Director of Customer Engineering at MasOrange

Javier Olveira holds a Telecommunications Engineering degree from the University of Vigo and a Master's in Operations Management from IE Business School.

With 25 years of experience in telecommunications and B2B markets, he has built his career around serving enterprise and public sector clients. He began at Comunitel before joining Orange in 2006, where he led large enterprise operations and customer engineering teams.

Today, at MasOrange, he is responsible for shaping the strategy and development of 5G and B2B technology solutions, overseeing both customer engineering and technology functions.

Thomas Sourdon

Director of Strategy and Competitiveness at Orange Business

Thomas Sourdon is a Senior Manager with over 25 years of experience in telecommunications, network engineering, and strategic leadership.

A graduate of IMT Atlantique and CCIE-certified, he has held various roles working directly with enterprise clients.

An expert in networks and a pioneer in SDN, SD-WAN, and SASE, he shifted to strategic consulting for diverse businesses.

Currently, he is Strategy and Competitiveness Director at Orange Business, focusing on transforming communication services into a platform-based model. His goal is to enhance network resilience and build trust amid evolving, complex enterprise challenges.

Explore more from The Kyndryl Institute
kyndryl.com/institute

The confidence to innovate

How resilience and trust power growth

Resilience is often perceived as slowing things down. The last hurdle before launch, the compliance box to tick, the over-engineered safety net that adds cost, delay and frustration. It's seen as the brake on innovation rather than the catalyst for it. But what if we reframed that thinking? Resilience is increasingly a strategic enabler: the force that propels organizations into new markets, ahead of competitors and onto faster, safer innovation cycles.

In many ways, the shifting business landscape makes this evolution in thinking unavoidable. Critical systems have moved to hyperscale clouds, reducing direct control. Cybercrime has matured into an industrial market, accelerated by AI. Geopolitical decisions now influence digital infrastructure in unpredictable ways. And the deepening of digitalization means a single point of failure can halt operations entirely. Disruption is a certainty; the difference is how we absorb and harness that disruption — and that's an intentional design matter."

Resilience in the darkness

Spain's national blackout in April 2025 illustrates the stakes. Power across the Iberian Peninsula collapsed after a chain reaction of voltage and stability issues within the grid, cutting electricity to tens of millions of people. Hospitals and other critical sites switched to emergency generators, isolated pockets of power where residents queued to charge phones, withdraw cash and access Wi-Fi as mobile networks faltered. Transport systems shut down. Airports and rail stations were immobilized. The Spanish government declared a state of emergency, such was the level of disruption.[1]

Large parts of the country remained offline for nearly 23 hours before the grid stabilized, but the operational divide between organizations was stark. Those with diverse connectivity, segmented systems, automated failover and embedded back-up power retained enough continuity to function. Those without stalled completely. The divide wasn't luck — it was design.

The technologies enabling modern resilience

Modern resilience comes from an architectural mindset rather than a single tool — one that assumes failure, absorbs it and recovers quickly. From a technology perspective, four key capabilities now define resilient organizations:

Platformization and infrastructure-as-code: Systems are treated as code, enabling rebuilds, rollbacks or redeployments in minutes. The platform encodes the intended state, a 'digital DNA', that allows systems to self-correct quickly and predictably.

Segmentation and fault-tolerant design: Failures are contained by design. Networks, workloads and data paths are isolated so incidents remain localized.

Zero-trust access: Identity-driven controls replace perimeter security, limiting what any user, device or service can touch. Collaboration becomes safer by default.

Defensive AI and automation: AI separates signal from noise across logs, networks and endpoints, allowing routine responses to be automated and human attention to be focused where it matters most.

These foundations transform recovery from emergency effort into routine operation.

How trust extends resilience against the unknown

'Trust' stands for an organization's ability to act predictably, securely and competently under any condition. Trusted infrastructure is one component of that trust, but the concept also includes governance, transparency, autonomous operations and the organizational maturity that ensures consistent behavior even in unforeseen scenarios. This trust rests on three pillars:'

1. **Control of the infrastructure** — the ability to reconfigure, reroute or replace components at speed.
2. **Autonomous operations** — owned tools, processes and teams able to act independently.
3. **Embedded security and resilience** — capabilities built into the fabric of operations, not layered on top.

> Resilience protects against the scenarios organizations plan for. Trust protects against the ones they don't...

Transparency is at the center of these pillars. Organizations need to know how systems are built, where dependencies lie and how risks are managed. Transparency gives customers confidence in the architecture supporting their business.

Lessons from the Iberian blackout

The Iberian blackout showed how extreme disruption can overwhelm even well-engineered resilience. The power loss didn't just take down local networks; it also disabled several coastal landing points that carry international traffic — routes used by major providers. These links are normally highly resilient, spread across multiple ports and protected by backup systems. What they weren't designed for was a country-wide outage that outlasted those backups and brought every route down at once.

This is where trusted infrastructure became the differentiator. Deep visibility and control of the infrastructure are practical expressions of trust: they give operators, including Orange, the ability to diagnose, reconfigure and recover systems quickly, demonstrating the competence, transparency and reliability that underpin organizational trust. In the case of the Iberian blackout, operators with this kind of infrastructure were able to re-engineer traffic through alternative landing points in France and activate alternative networks to bypass the outage. Performance reduced, but continuity returned within hours. Others without that level of operational autonomy had no option but to wait for the grid to recover.

The blackout also reset design assumptions. Recovery playbooks were revised, landing diversification widened beyond Spain, and national-scale power loss was added to baseline engineering so future routes avoid concentration risk.

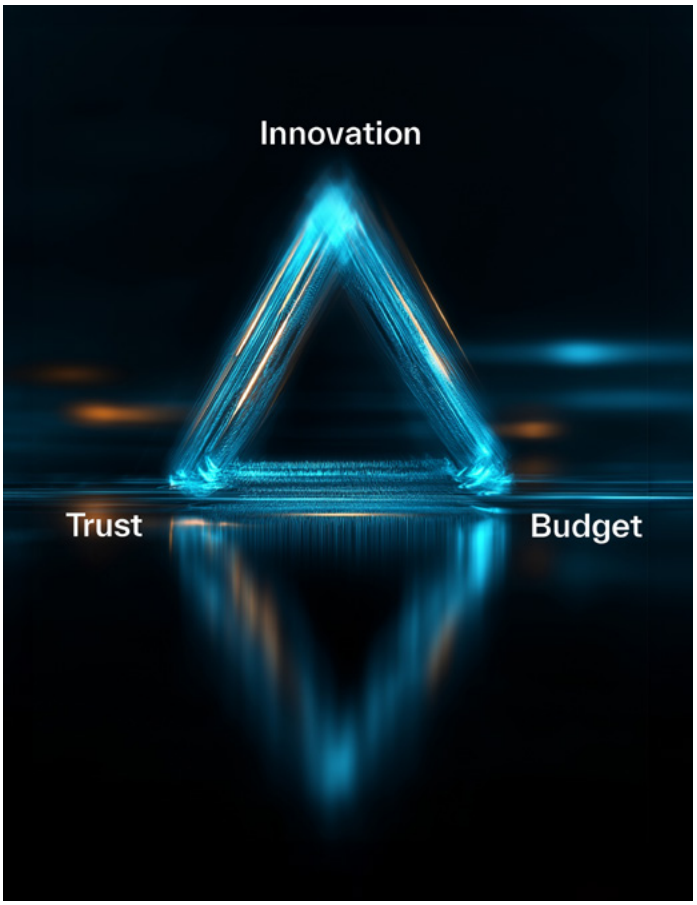
It is important to say that trusted infrastructure doesn't prevent every disruption, but it ensures organizations retain the ability to respond and recover when resilience alone is not enough.

Calibrating trust: the innovation–trust–budget triangle

While the need for trust is clear, there is also a question of how much to apply. Increasing trust reduces operational risk, but may require higher cost or slower change, while reducing trust can accelerate innovation but increases exposure.

Every organization operates inside a triangle defined by innovation, trust and budget. No company can maximize all three at once, so the task is to decide the right point on that triangle for each part of the business.

Modern, software-based platforms make these trade-offs feasible. They provide a baseline of security and resiliency with the option to increase trust where it matters, while accepting the cost and agility implications. Equally, when innovation speed is the priority, the platform's ability to switch between technology providers and services limits lock-in and makes bold choices reversible rather than a one-way bet.



In practical terms, this calibration shows up in how services are designed and delivered. Some organizations choose higher-assurance configurations — for example, hosting key management functions in their own facilities or in a dedicated environment provided by their operator. This gives them greater control and independence, but comes with higher cost and a slower update cycle because every new software release must be validated first. Others prioritize agility and lean into shared, cloud-based options where innovation arrives faster. Because modern platforms allow components to be swapped like-for-like, organizations can avoid lock-in and respond quickly to price changes, end-of-life announcements or performance concerns.

Sector expectations also shape these decisions: most organizations are comfortable with shared infrastructure when transparency is high. But financial institutions, for example, often keep sensitive elements within their own facilities.

The triangle therefore becomes an operating dial. Organizations tune trust to risk, tune speed to ambition and tune cost to budget — all enabled by a transparent platform that makes those trade-offs deliberate rather than accidental.

Making innovation safer, faster, bolder with resilience at the core

Innovation inevitably brings uncertainty: unfamiliar behaviors, untested interactions and emerging threat surfaces that cannot be fully predicted in advance. Without the right foundations, those uncertainties force organizations to slow down, adding process and caution to compensate for architectural gaps. But **when resilience and trust are embedded into the foundations of the platform, that dynamic shifts entirely**. Guardrails are already in place, making it safe to launch earlier. Rollback is effortless, making iteration cheap. Segmentation and zero-trust keep missteps contained, limiting the impact of error or attack. Systems regenerate their intended state automatically, turning recovery into an expected, near-instant action rather than a complex intervention. Even collaboration becomes safer, with identity-driven controls enabling openness at the edge while protecting what matters at the core.

When the innovation–trust–budget triangle is calibrated with intention, innovation becomes a governed, repeatable engine of progress rather than a gamble.

Reference

1 Blackout in Spain and Portugal 'first of its kind', report finds, BBC News and How Spain powered back to life from unprecedented national blackout, BBC News