Softtek®

2026 EDITION

CIO Agenda

2026 EDITION

The CIO as a Digital Business Innovator

CIOs shift from technology operators to accountable drivers of enterprise value

In 2026, a shift that many CIOs intuited, but which now becomes inescapable, is consolidated: **the conversation stops revolving around technological experimentation and focuses on economic responsibility**.

The question is no longer what we can prove, but what return each investment generates and what risks the organization assumes by scaling it. This shift is driven by diverging forces:

Forces driving change

The ai market enters a correction phase

After a stage of accelerated enthusiasm, **many organizations are struggling to translate use cases** into sustained financial impact

The risk surface reconfigures

The World Economic Forum ranks **digital fraud among the most widespread threats** and elevates it to the level of senior management

The world activates a new wave of regulatory enforcement

With more provisions of the AI Act coming into force, **AI becomes a matter of compliance, accountability and executive traceability**

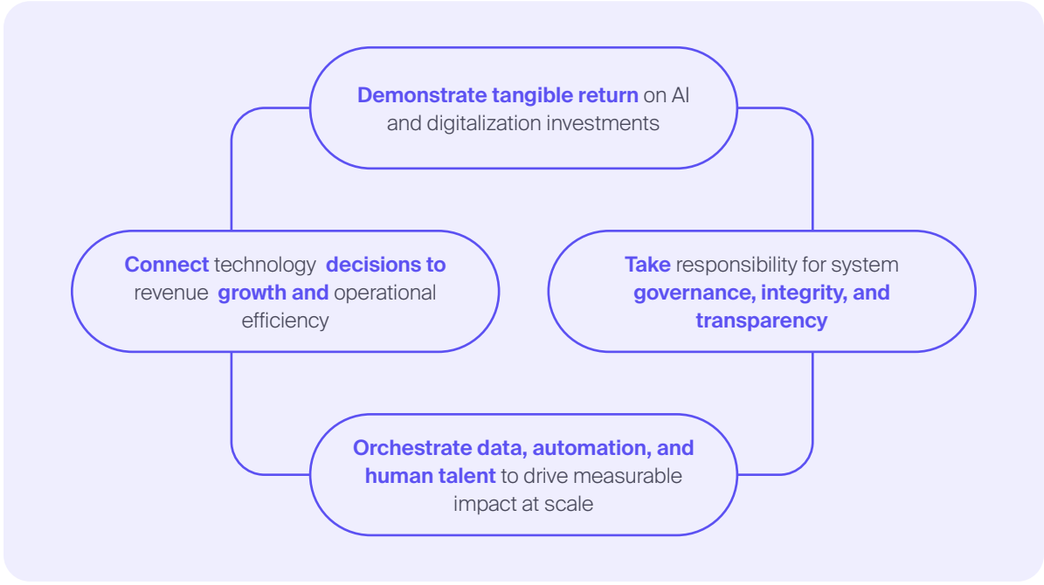
Economic pressure not diminishing

57% of CIOs report **direct pressure to improve productivity,** and 52% to reduce costs

Source: Gartner

Technology, especially AI, **is no longer a support function and is consolidated as the main driver of growth**, efficiency and competitive differentiation.

It cannot remain encapsulated in IT and, above all, must be integrated into the design of the business model. Therefore, today, the CIO is expected to:



Two or three years ago, the debate was technical and exploratory, **in 2026, it is strategic and financial**. This implies a profound transformation of the executive positioning.

The CIO must work closely with the CEO and CFO on capital allocation decisions. Investments in AI and digital platforms are no longer approved for technical sophistication, but for expected return, scalability, and risk profile.

At the same time, it **operates in a constant friction between the demand for immediate results and the obligation to innovate** to sustain future competitiveness, budgetary pressures from the CFO and regulatory requirements that require demonstrating software integrity, data authenticity and transparency in automated decisions.

Postponing priorities, delaying scalability or avoiding assuming regulatory responsibility has **a direct impact on budget, reputation and strategy**.

Technology decisions now directly determine growth, margin, and resilience

For years, the CIO's mandate was clear and relatively stable: ensure the availability of infrastructure, applications, and networks, maintain adequate levels of security, meet budgets, and ensure operational continuity. Success was measured in technical metrics, and the IT function operated as a reliable, efficient, and predictable cost center, but with limited influence on product, revenue, or competitive positioning. **That model was not wrong, it responded to an environment in which technology enabled the business, but did not define it**.

In 2026, that mandate will prove insufficient. **The competitiveness of organizations now depends on structural digital capabilities**. Data, platforms, software, and artificial intelligence don't support the operating model from the back-office, they now set it up. Customer experience, process efficiency, speed of new product launches, and the ability to manage risk are all directly influenced by technological decisions. Therefore, technological architecture ceases to be an internal issue and becomes a strategic determinant.

In this scenario, technology becomes the direct engine of growth, margin, and resilience. Data strategy is, in practice, organizational strategy. Automation and AI influence critical decisions, and the ability to transform information into economic impact becomes a tangible competitive advantage. As a consequence, the CIO is no longer evaluated exclusively by the quality of technical execution and begins to be measured by business results. Today, virtually all CIOs report to the board on return on technology investment, and **more than 90% are actively involved in defining corporate strategy**.

The CIO, therefore, acts as a co-responsible for the value by sharing decisions that affect the P&L, influencing the allocation of capital and participating in the definition of strategic priorities, trying to co-design the economic model of the organization with the rest of the managers. This shift explains why the traditional boundaries between CIOs, CTOs, and business areas are blurring. Investment priorities, platform selection, architecture definition, and risk management cannot be solved in silos. The CIO becomes an orchestrator: he integrates technical capabilities, growth objectives, and financial constraints to make coherent, defensible, and sustainable decisions.

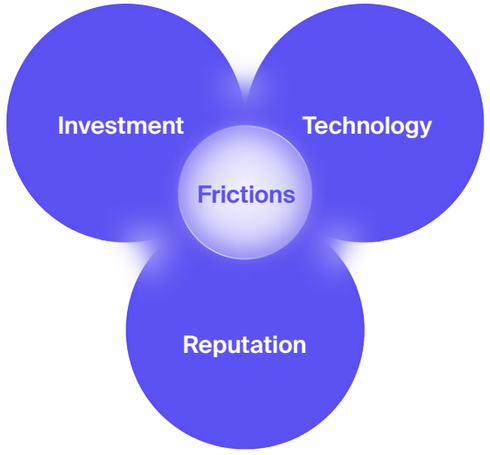
The metric of success also changes. In 2026, **technology is evaluated for its impact on digital revenues, margin improvement, structural cost reduction, productivity, time to market, and demonstrable resilience.** Budget pressure, the real cost of scaling AI, and increased regulatory risk force us to abandon the logic of permanent experimentation and adopt a rigorous discipline of prioritization.

CIOs from now on do not lead by what they know about technology, but by the economic decisions they are capable of making; decisions about what to promote, what to scale, what to simplify, and what to abandon.

Sources: Logicalis | Fortune | PR Newswire | Lighthouse

Competing financial, technological, and regulatory pressures force unavoidable trade-offs

Exercising the role of CIO as a results manager today becomes complex because **the forces that affect the technological function have intensified simultaneously and, in many cases, in opposite directions**. Economic pressure, ambition for innovation, regulatory tightening, architectural complexity and organisational frictions converge without offering comfortable room for manoeuvre. The result is greater demand, along with a permanent structural tension in which every decision, and every delay, implies a real trade-off for the business.



1. Investment

- Immediate ROI is required on investments that require long-term maturation.
- Finance assesses as a cost what technology proposes as a strategic investment.

2. Technology

- Platform stacking reduces visibility and increases operational risk.
- Integrating legacy systems with AI consumes more resources than innovating.

3. Reputation

- AI Expansion Moves Faster Than Control Models.
- Responsibilities for AI risks are not clearly assigned.

Investment

The first friction is economic, **more than eight out of ten CIOs recognize direct pressure to justify the return of AI in increasingly shorter horizons**, precisely when its adoption requires relevant initial investments in infrastructure, data, talent and operational redesign. Although the relationship between CFO and CIO is mostly described as collaborative, **almost half admit friction in the evaluation of return and more than a third in budget allocation.**

Technology

The second source of tension is the complexity they generate. **AI adds layers of architecture, critical data dependencies, and governance demands that multiply the difficulty of operating** securely at scale. Added to this is the proliferation of tools and suppliers.

Most organizations operate with multi-vendor ecosystems and a large number of professionals recognize that poor integration slows down incident response. The accumulation of solutions, far from providing control, often translates into less visibility, hidden costs and a widening of the risk surface. Scaling intelligent capabilities and containing exposure and complexity becomes a delicate exercise. On the one hand, consolidating reduces friction and cost, but it can be perceived as a loss of autonomy. On the other hand, maintaining diversity preserves apparent agility, but increases vulnerability.

Reputation

A strict regulatory and reputational environment is superimposed on these. **The demands in terms of data, AI and digital sovereignty force us to strengthen controls just when the business demands speed**. A majority of CFOs prioritize strengthening reporting and oversight before expanding the use of advanced AI. AI has intensified collaboration between finance and technology, but it has not fully clarified responsibilities. Only a minority of organizations claim to have fully defined governance schemes around AI, precisely when the associated risks are most difficult to reverse once deployed.

By 2026, it has become clear that **proliferation generates redundancies, increases support costs, and sucks energy out of teams, which spend more time sustaining the ecosystem than transforming it**. Technical and data debt is quietly piling up, while the promise of simplification associated with cloud and AI coexists with increasingly dense architectures. The CIO is thus faced with the task of re-optimizing and re-architecting in order to scale reliably.

Strategic priorities persist, but the execution bar rises

The priorities that were foreseen in 2025 are not redefined by substitution, but by maturity. What was presented as a strategic opportunity, differentiation or technological exploration, **in 2026 becomes an executive requirement under explicit criteria of scale, control and return**.

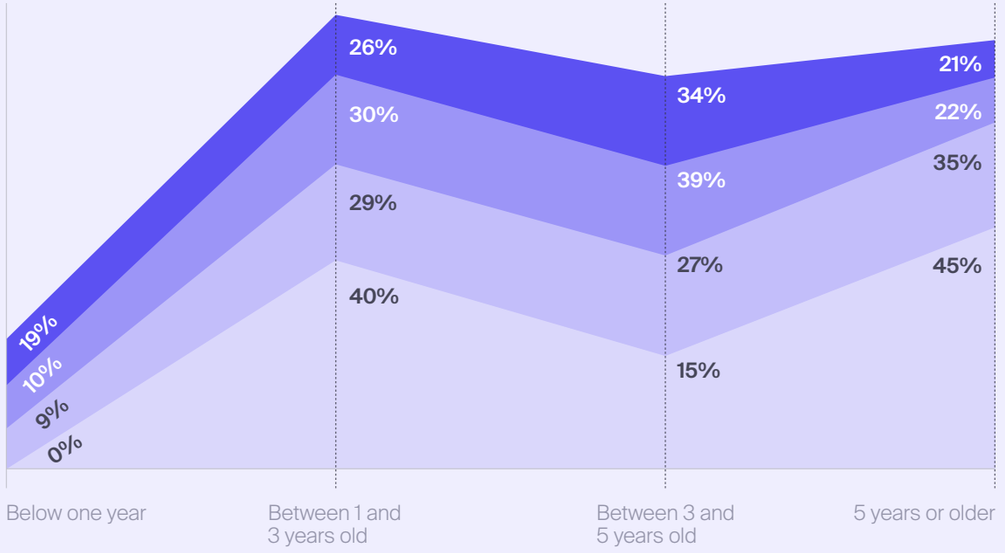
The environment, in reality, has not changed in the topics, but in the conditions under which they can be addressed. Organizations have already invested massively in AI, advanced analytics, cloud architectures, and accelerated innovation models, and these capabilities have shifted from aspirational to the strategic core of most companies. For this reason, **the debate turns from whether to invest in technology (because practically all of them are doing so) to what real impact these investments generate and at what organisational, economic and reputational cost**.

The magnitude of the effort is indisputable. The vast majority of organizations allocate technology resources to create new revenue streams, and AI spending maintains double-digit growth rates. However, as investment increases, the gap between adoption and impact also becomes more visible: **only a minority of initiatives manage to capture the expected return and only a fraction manage to scale at the corporate level**.

As many as 85% of CIOs acknowledge direct pressure to demonstrate tangible impact, and a similar proportion say that the return of AI is already under explicit scrutiny. As a result, technology is no longer measured by sophistication or volume of initiatives and is measured by its verifiable contribution to growth, margin, and resilience.

At the same time, **the context has hardened on the different fronts** that cross all digital decisions and that explain this change in status without the need to redefine priorities:

Roi expectations for the highest level of automation with AI extend more than three years

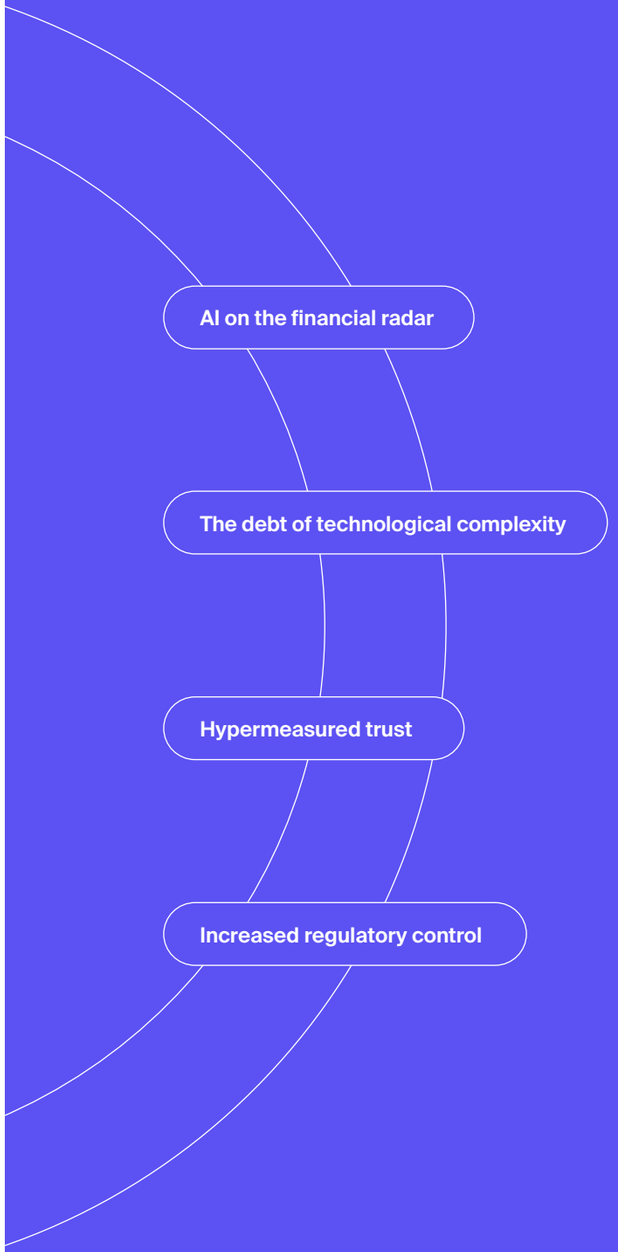


Only 25% of AI initiatives have delivered the expected ROI in the last three years

Sources: PR News Wire | Logicalis | CIO.com | IBM

All these facts **mean that the trends that drove the agenda during 2025 remain strategic, but lose their aspirational character**. They no longer justify attention by themselves nor can they be approached from the logic of permanent exploration.

Priorities are reread from this new reality, to show how they evolve from possibility to enforceable obligation. Through four blocks that group the challenges assessed last year: advanced AI and experience, innovation and speed, governance, platforms and reliability, and data, ecosystems and regulation, it **will be analyzed how the focus shifts from adoption to responsibility for scale**.



Dimensions of change

1. AI now competes for capital under criteria comparable to any other strategic investment, which forces it to justify its economic viability
2. Platform proliferation and tool overlap represent operational inefficiency and impact speed of execution, risk visibility, and ability to scale
3. Tolerance for error is reduced, technological incidents impact reputation and value, and the requirement to demonstrate control, traceability and responsibility is installed at the executive level
4. GDPR, DORA, NIS2 or the AI Act introduce requirements on data, resilience and high-risk models that affect architecture, governance and responsibilities at the C-level

Sources: PR News Wire | Logicalis | CIO.com | IBM

AI investment is justified only when scalable, governed, and economically defensible

The hardening of AI's promise

IA multimodal | Digital twins | Emotional computing | GenAI models

In the previous CIO Agenda, **the conversation about advanced AI revolved around its differentiating potentia**l. Multimodality, digital twins of the customer, affective computing or innovation assisted by generative models were presented as levers capable of enriching decision-making, hyper-personalizing the experience and automating processes on a large scale.

That ambition has not been diluted, on the contrary, the intention to adopt confirms it. Today, 44% of customer service leaders are exploring conversational generative AI and 11% are in the pilot phase, reflecting a **sustained interest and a real willingness to incorporate these capabilities into the operational core**.

However, the distance between intention and scale is significant. Only 5% have managed to deploy solutions structurally and only 16% of AI initiatives manage to scale to the entire organizational level. In other words, **technological sophistication is advancing rapidly, but its industrialization comes up against structural barriers linked to data, architecture, processes and governance**.

In 2026, AI applied to experience is no longer legitimized by its level of sophistication and is now evaluated as an executive decision that combines investment, risk and reputation. Funding is no longer based on technological promise, **but on the ability to demonstrate scalable return, while the transition from pilot to production requires resolving structural dependencies** and redesigning processes beyond the isolated experiment.

Mass exploration, on its own, has ceased to differentiate. **The real competitive advantage now lies in the ability to select judiciously, prioritize with discipline and scale consistently** those initiatives that generate measurable and defensible value over time. What was previously interpreted as leadership due to technological sophistication becomes, in 2026, an explicit demand for economic impact, discipline of scale and formal responsibility.

Why the focus changes

44% of customer service leaders **explore generative AI**

11% are in pilot and only **5% have deployed it significantly**

Only 16% of AI initiatives **manage to scale to the full organizational level**

Previously, advanced AI represented a differentiation lever based on technical capacity and accelerated exploration, **now it only justifies investment if it demonstrates scalable returns, formal governance and real industrialization capacity**

The AI scaling requirements

1. **Required Return**
   Financing conditional on scalable ROI
2. **Complex scale**
   Industrializing AI overcomes isolated pilot
3. **Regulatory Responsibility**
   AI subject to formal obligations
4. **Measurable impact**
   Economic results replace experimentation

Sources: Forbes | CDO Magazine | Makebot AI

Speed loses advantage when innovation fails to industrialize at scale

The end of indefinite experimentation

Accelerated prototyping

Dynamic ROI measurement

Last year, the focus was on **accelerated prototyping and dynamic ROI measurement as tools to reduce time-to-market and learn before the competitor**. The logic was to iterate quickly, adjust on the fly, and capture advantage from agility.

However, the results have introduced a less optimistic nuance. Only 48% of digital initiatives meet or exceed their business goals, which means that **more than half fail to realize the expected value**.

This mismatch coincides with a clear tightening of the financing logic. Today, 72% of CFOs lead the technology budget and, in 41% of organizations, they are directly involved in decisions about which technology is acquired. Added to this is an explicit expectation of tangible return in horizons of 12 to 18 months, which reduces the margin for open initiatives without a clear trajectory towards results.

Financial pressure is **amplified by a structural constraint: accumulated technical debt**. More than 90% of leaders recognize that their organization carries significant technological burdens and nearly 80% admit that these have caused cancellations, delays or cost increases in critical projects.

The competitive differential in 2026 lies not in multiplying experiments, but in **exercising greater selectivity and transforming a limited set of initiatives into scalable**, governed, and financially defensible products.

CIO leadership evolves accordingly. Rather than enabling a growing volume of pilots, it is now a matter of **orchestrating a disciplined portfolio of innovation, with explicit criteria of priority and accountability shared with business and finance**, where the quality of execution weighs as much as the originality of the idea.

Why the focus changes

72% of **CFOs lead** the technology budget

41% **decide which technology to buy**

More than **90%** of organizations admit to **carrying technical** debt and nearly **80%** admit that it has already **delayed or canceled key initiatives**

Previously, innovating faster than the market was a sign of digital maturity, today, **speed loses legitimacy if it does not translate into scalable, financially defensible and sustainable products** in architecture

The new rules of innovation

Innovation logic
Speed ceases to be objective and becomes a condition

Success Metric
Only initiatives with a clear path to industrialization survive

Operating model
Distributed experimentation gives way to prioritized portfolio

Governance and financing
Innovation is financed under investment logic, with clear expectations

Organizational culture
The "fail fast" culture evolves towards "scale responsibly"

Sources: Service Path | Market Screener | unqork AI | II

Resilient platforms become mandatory infrastructure for sustainable innovation

The fragility of accumulated complexity

Product Governance

Predictive observability

In the previous Agenda, the conversation on governance and platforms was articulated around **digital product governance and predictive observability as instruments to scale coherently and anticipate risks**.

In 2026, the expansion of AI, autonomous agents, and advanced automation has substantially increased the interdependence between systems, data, and processes, **increasing the systemic risk associated with any failure**.

What could previously be managed as a localized incident today has the capacity to propagate with operational, financial and reputational impact.

The underlying architecture reflects this accumulated fragility, 70% of organizations operate with multi-vendor environments in cybersecurity and stacks that, in some cases, exceed 70 different tools. In addition, 43% of professionals acknowledge that a lack of integration consumes critical time and **36% admit that complexity makes it difficult to respond quickly to threats**.

Exposure data confirms the magnitude of the risk: more than 80% of organizations have suffered multiple breaches in the last year and the average cost of an incident in critical sectors exceeds five million dollars. **Resilience, therefore, becomes a direct variable of the business**, linked to operational continuity, customer confidence and financial stability.

Therefore, in 2026, architectural standardization, vendor consolidation, and the integration of security and compliance by design are not optimization options, but **necessary conditions to scale AI and automation without amplifying the fragility of the system**.

The CIO's focus is thus shifted from reactive control to the **deliberate construction of a coherent and reliable technological base**, on which innovation can grow without multiplying structural risk.

Why the focus changes

72-74% of organizations operate with **multi-vendor stacks in cybersecurity**

More than 80% of organizations have suffered multiple **breaches in a 12-month period**

36% recognize that complexity **hinders speed in the face of threats**

Governance was understood as a mechanism to order digital expansion. Now, the scale achieved by automation and AI shows that **without a resilient technological base, expansion becomes fragile**

The structural conditions of the scale

Total interdependence of the digital environment

Technological decisions now **impact the entire** operational, financial and reputational chain of the company

Complexity that exceeds the functional threshold

The accumulation of suppliers and layers causes **fragmentation to begin to limit responsiveness**

Permanent exhibition with no margin for error

The gaps, detection times and economic impact show that **continuity cannot depend on subsequent controls**

Legacy base that conditions future scale

Technical debt reduces the ability to absorb burdens and makes **standardization a prerequisite for growth**

Sources: Daily Security Review | Petri | IBM

Data creates value only when its use is traceable, defensible, and compliant

The data under permanent scrutiny

Open data ecosystem

Strategic Compliance

In the previous Agenda, data ecosystems and multi-sector collaboration were presented as natural accelerators of personalization, efficiency, and new business models. **Data was conceived as an asset whose value increased as it circulated and was combined**.

That ambition does not disappear, but its viability is subject to new conditions. In increasingly interconnected environments, where data flows between organizations, platforms and intelligent models, the question is no longer only how much can be exploited, but **under what guarantees this use can be sustained over time**.

The investment confirms its centrality: 74% of executives prioritize real-time data infrastructures and 86% plan to increase spending on data management, with an explicit focus on privacy, security and governance. However, **62% identify gaps in data governance as the main obstacle to scaling AI and automation**.

Added to this internal gap **is a regulatory framework that ceases to be declarative and becomes operational**. The new regulations do not act outside of digital business, but condition it from its design: they impact contracts with third parties, information classification, data architecture and model development.

The pressure, moreover, is economic. Between 75% and 80% of consumers report reducing or abandoning their relationship with a brand after a data breach, and nearly half avoid signing up for services that have suffered recent incidents. **Digital trust thus translates into tangible economic behavior, affecting revenue, retention, and positioning**.

In this context, the CIO ceases to be only an enabler of analytical exploitation and **assumes the role of guarantor of the defensible use of data**, articulating value, compliance and trust as inseparable dimensions of the same strategic architecture.

Why the focus changes

>75% of consumers **abandon brands after a breach** = 50% avoid signing up for services with **recent incidents**

Organizations prioritize:

43% investment in **privacy and security**

41% investing in data **governance and AI**

In the past, data ecosystems were conceived as a lever for collaboration and innovation, today, **data only generates value if its use is defensible, traceable and robust in the face of regulation, partners and the market**

The data legitimacy circuit

1. **Expanding the Data Ecosystem:** They flow between partners, platforms, and models. The greater the interconnectedness, the greater the dependency as a strategic asset
2. **Regulatory and contractual intensification:** Frameworks such as NIS2, DORA or AI Act introduce formal obligations, condition architecture, contracts and classifications
3. **Gap between analytical ambition and governance:** Analytics outweighs governance capability, and when AI scales on poorly structured data, risk multiplies
4. **Direct impact on confidence and growth:** Digital trust directly influences customer behavior and brand reputation. The data can erode growth

The CIO's New Mandate: 7 Challenges for 2026

From strategic signals to executive decisions

The issues that have occupied the CIO's agenda in recent years do not lose value in 2026. Artificial intelligence, architectural modernization, data governance, operational efficiency, and talent transformation continue to be structural axes of technological leadership. However, what changes substantially this year is the level of specificity that is required regarding its execution and its impact.

The environment has hardened expectations:

- The **promise of AI has ceased to be aspirational** and has become a demand for results.
- **Indefinite experimentation has exhausted its legitimacy** and the market no longer grants unlimited time to learn without demonstrating value.
- The **complexity accumulated over years of technological growth is beginning to show its structural fragility**.
- The **data operates under constant scrutiny**, both regulatory and economic.

The gaps identified last year can no longer be interpreted as part of the maturation process and, **in 2026, become decisions that must be made clearly**.

In this context, **the relevance of the CIO will depend on his ability to translate ambition into structure, innovation into scale, and technological deployment into strategic legitimacy**. Impacting internally implies reinforcing the structural foundations on which the organization operates, simplifying architectures, integrating governance from design and ensuring operational coherence. On the other hand, having an external impact requires demonstrating that technology contributes in a tangible way to the margin, growth and resilience of the business.

The 2026 Agenda is structured around three vectors:

1 Structural foundations

Strengthen technology coherence, simplify architectures, integrate governance by design, and consolidate data as a strategic asset, ensuring that the organization can operate with robustness, resilience, and clear standards

2 Scaling mechanisms

Tramsform innovation into sustained productive capacity, installing investment discipline, explicit productization criteria and operating models that allow technological ambition to be converted into verifiable return

3 Strategic legitimacy

Consolidate the position before the CEO and the Board, redesigning the organizational model and adopting metrics and narratives that connect technology with margin, growth and business resilience

The CIO's new challenges in 2026

In 2026, CIO leadership will be measured by their **ability to rigorously prioritize, sustain, and validate impact**.

Only in this way will it maintain its relevance throughout the year and **consolidate its position as a strategic architect of the business**.

Challlenge#1 Structural Foundations

Simplify and unify the technology ecosystem to scale

Over the past few years, digital expansion and the pressure to accelerate capabilities have pushed many organizations into a recurring pattern, solving one-off needs by adding tools, not redesigning the system. The result, in addition to a larger stack, **is a fragmented ecosystem where vendors, overlapping platforms, and custom integrations proliferate**.

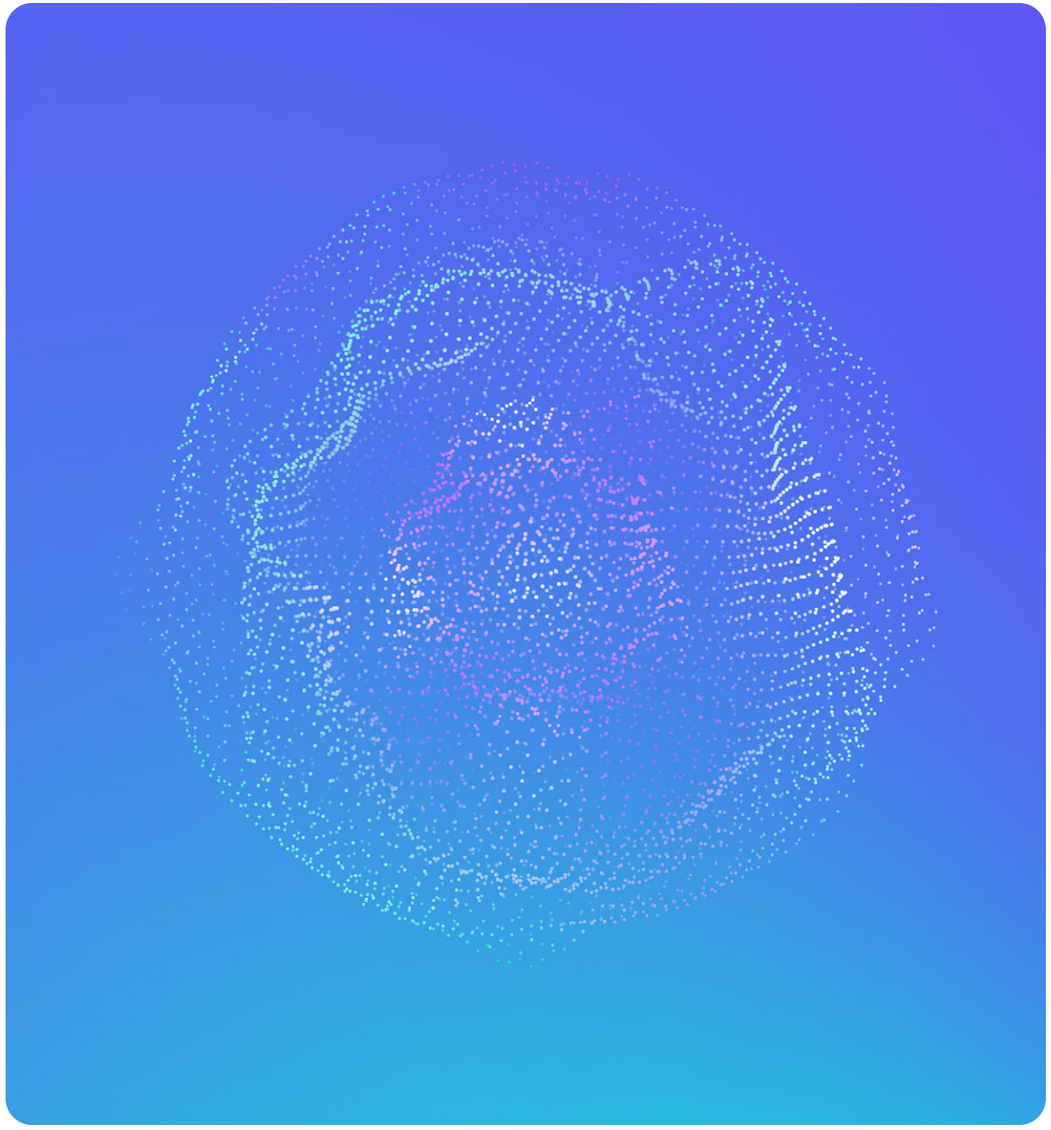
In some environments, reality is close to a museum of tools, with **dozens of solutions coexisting, with uneven levels of use, partial governance and a limited understanding** of the total cost of operating them.

The first effect of this fragmentation is a direct erosion of operational capacity. Most organizations today operate with multi-vendor approaches and a substantial portion of teams admit that the **environment has become too complex to manage efficiently**.

That complexity becomes constant friction: time consumed by poor integrations, functional duplication, lack of end-to-end visibility, and technical decisions that rely on the tacit knowledge of few experts. As the stack grows, **the organization gains tools, but loses coherence, and consistency is the prerequisite of scale**.

The second effect is the invisible cost. Much of the technology spend comes from integrations, maintenance, APIs, identity management, incident resolution, and cross-team support. In many cases, **integration ends up costing several times as much as the tools themselves, and it is sustained year after year as a structural burden**. This explains why, even after modernization programs, a high proportion of the IT budget is still spent on "keeping the lights on.

The third effect is that, paradoxically, the growth in the number of tools does not always improve the control posture. More platforms and vendors mean **more points of failure, configurations to maintain, shelfware risk, and a larger attack surface**.



Challlenge#1 | Structural Foundations | Simplify and unify the technology ecosystem to scale

In 2026, this dynamic is no longer tolerable as AI amplifies the fragility of the ecosystem. **Intelligence needs seamless integration, consistent data, and consistent observability to scale**. When architecture is fragmented, AI becomes an additional layer of complexity: models disconnected from reliable data, pilots that don't industrialize, automations that can't be governed, and results that are difficult to replicate.

That's why many organizations remain stuck in the pilot phase, not because of a lack of ideas, but because **the system doesn't support the transition from experiment to operation**.

The hidden cost of fragmentation

Challlenge#1 | Structural Foundations | Simplify and unify the technology ecosystem to scale

The answer is not to execute an indiscriminate cut, but to adopt a different logic, moving from accumulating tools to designing an intentional ecosystem. **Simplifying and unifying is a structural decision to regain speed, resilience, and scalability**. While a fragmented stack grows by aggregation, a strategic platform grows by consistency.

That's why the CIO's first move is to change the type of internal conversation. The question is no longer what tool we are missing and becomes what part of the ecosystem is duplicated, what it integrates badly, and what hidden cost we are sustaining. **This transition forces us to make uncomfortable but inevitable decisions that almost no organization makes explicitly.** In practical terms, simplifying means reducing surface area, not only in cost, but also in operation and risk.

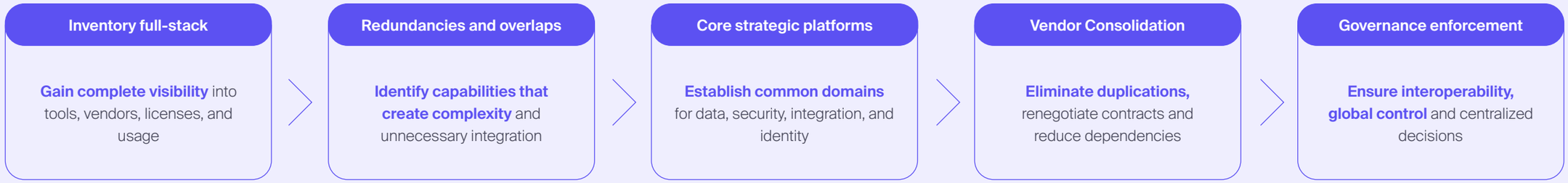
A robust approach for this year is to sort consolidation by layers and by domains. Layered, because unifying requires clarity on where the data resides, how the operation is orchestrated, and how capacities are consumed in channels and applications. And by domains, because not everything deserves the same level of standardization, there are categories that must be governed as critical infrastructure, and others where autonomy can exist within explicit limits. **Centralizing the critical and limiting freedom in the peripheral allows reducing duplication without suffocating the business**.

Unification, moreover, must be translated into concrete capabilities that the CIO can govern and measure:

- In **architecture**, it involves **defining core platforms**, non-negotiable interoperability standards, and a clear catalog of permitted technologies.
- In **governance**, it requires a **formal evaluation process** to prevent the organization from falling back into the pattern, and explicit rules for handling exceptions.
- In **economic discipline**, it requires **full visibility** into licenses and actual usage, and into the cost of integration and maintenance.
- In **preparation for AI**, it implies that data and observability must be **fully integrated with each other**.

This challenge also repositions the relationship with the Board, simplification allows for clear reporting: fewer critical tools, more end-to-end visibility, better response times, and a system capable of sustaining automation and AI without multiplying risk.

From fragmented stack to unified strategic platform



Challlenge#1 | Structural Foundations | Simplify and unify the technology ecosystem to scale

HOW IT IS ACHIEVED

Turning simplification into corporate discipline

Simplifying and unifying an organization's technology ecosystem is achieved when the CIO succeeds in transforming simplification into a corporate program with economic legitimacy, financial backing, and sustained architectural discipline. It is necessary, for this, to change the framework of the conversation until now. As long as simplification is perceived as a technical initiative, it will compete with business priorities and be interpreted as a constraint.

With the CFO leading the technology budget in most organizations, consolidation cannot be executed as a unilateral agenda. The CIO achieves the challenge when he turns architecture into a financial criterion. This implies that technology investment decisions are subject to explicit rules: evaluation of the total cost of ownership, including integration and operation, functional redundancy analysis and validation of alignment with the target architecture.

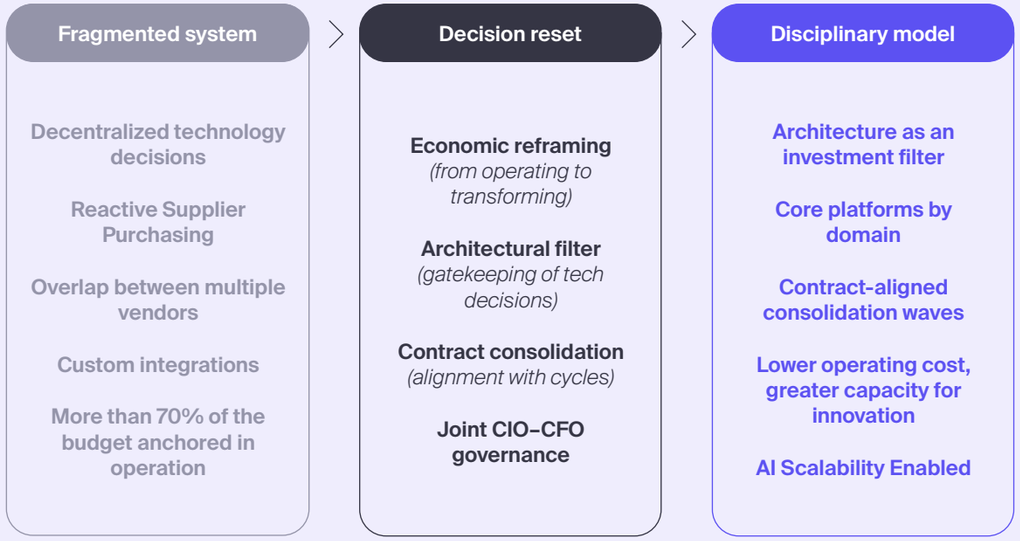
Execution, however, must recognize the actual constraints. Effective simplification is designed by aligning consolidation with contractual windows, budget cycles, and volume renegotiations.

In other words, waves must be planned that combine the elimination of obvious redundancies, progressive consolidation of core platforms and structural negotiation with dominant vendors.

At the same time, the legitimacy of the program depends on demonstrating early impact on the fronts of greatest concern. Therefore, the process should start with the domains where the sprawl locks critical value.

Reducing tools in these layers decreases operational expenditure but also reduces attack surface, improves visibility and unlocks scalability of artificial intelligence initiatives.

The reset of the technological decision



The challenge is consolidated when **simplification is no longer perceived as a project and becomes a permanent discipline**. This requires institutionalizing a joint governance mechanism between CIO and CFO, which evaluates new technological additions under consistent architectural and economic criteria.

The CIO manages to simplify and unify the ecosystem when he manages to redesign the organization's technological decision system. It is a matter of establishing a logic in which each incorporation or permanence is justified by its contribution to a coherent, financially sustainable and ready-to-scale architecture.

Challlenge#2 | Structural Foundations

Sanitizing critical data before demanding results from AI

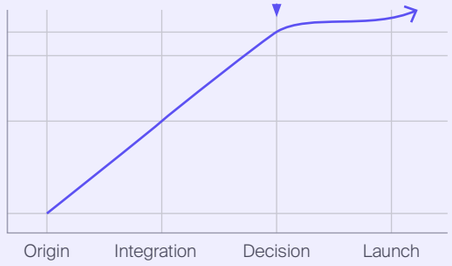
Until now, data quality has been treated as a technical problem: cleanliness, normalization, standardization. But, in 2026, this narrative is insufficient. Now, the flawed data is no longer an operational inefficiency, it is a direct economic risk. The figures show that **the average cost of bad data is around 12.9 million dollars per year per company, and different estimates place its impact between 15% and 25% of potential revenues**.

When these domains fuel human decisions, the impact is already significant, but when they fuel automated decisions, the impact is amplified. **AI ends up escalating inconsistencies**. A model trained on incomplete or contradictory data does not simply generate statistical noise: it generates biased recommendations, erroneous forecasts and automated decisions that directly affect margin and risk.

More than 50% of organizations identify data quality and availability as the main barrier to scaling AI, even above skills or regulation. And yet, few quantify this risk as a priority economic variable. ROI is demanded of AI while tolerating a base that, according to multiple estimates, erodes up to a quarter of potential revenue.

Data quality multiplies the cost of decisions

The cost of correcting an error increases exponentially when it has already been incorporated into decision processes



This cost materializes in erroneous decisions, rework, risks and loss of credibility. The later action is taken, the lower the ability to control and the greater the economic impact

Sources: TASMAN | Gyde | Amzur | IBM | Forbes | II | AI Data & Analytics Network

Challlenge#2 | Structural Foundations | Sanitizing critical data before demanding results from AI

There is also an exponential dynamic that aggravates the problem, where correcting errors at source has a marginal cost. **Modifying them when they have already fueled strategic decisions can multiply that cost to a great extent**.

That is why, **as AI is integrated into critical processes** such as credit approval, dynamic pricing or demand planning, **the impact of poor quality is no longer operational and becomes financial and reputational**. Trying to scale intelligence on unhealthy critical domains is tantamount to institutionalizing error.

Economic impact of data quality on AI

Data quality and governance	AI-based decisions and financial impact
Liability	Automatic pricing
Consistency	Risk assessment
Traceability	Demand Forecast
Quality metrics	Revenue Optimization
Standards	

AI amplifies the quality of the data it consumes

Sources: TASMAN | Gyde | Amzur | IBM | Forbes | II | AI Data & Analytics Network

Challlenge#2 | Structural Foundations | Sanitizing critical data before demanding results from AI

Sanitizing internal data means adopting a selective and economical logic, where domains in which error destroys the most value are prioritized and end up being treated as strategic assets. **The first must is to identify precisely which domains impact revenue and risk**, not all data deserves the same level of intervention: customer, pricing, inventory, risk, forecasting or fraud directly impact revenue, margin and financial exposure. These are domains where an inconsistency does not remain at the analytical level, and can affect automated decisions that are executed at high speed.

The second is **to assume that quality needs explicit accountability**. As long as data is perceived as a byproduct of transactional systems, its consistency will depend on tacit agreements and goodwill. When a critical domain has a clearly defined owner, with authority and responsibility for its consistency, traceability and evolution, the data ceases to be a technical abstraction and becomes a managed asset. Success in this area is mostly organizational, without clear accountability, debt accumulates silently

The third is **to introduce "quality gates" before the deployment of AI**. The organization cannot aspire to scale automation without verifiable standards. Consistency, completeness, timeliness, uniqueness, and traceability must be translated into explicit metrics and thresholds. **With defined metrics, the data is evaluated with the same discipline as any other strategic asset**.

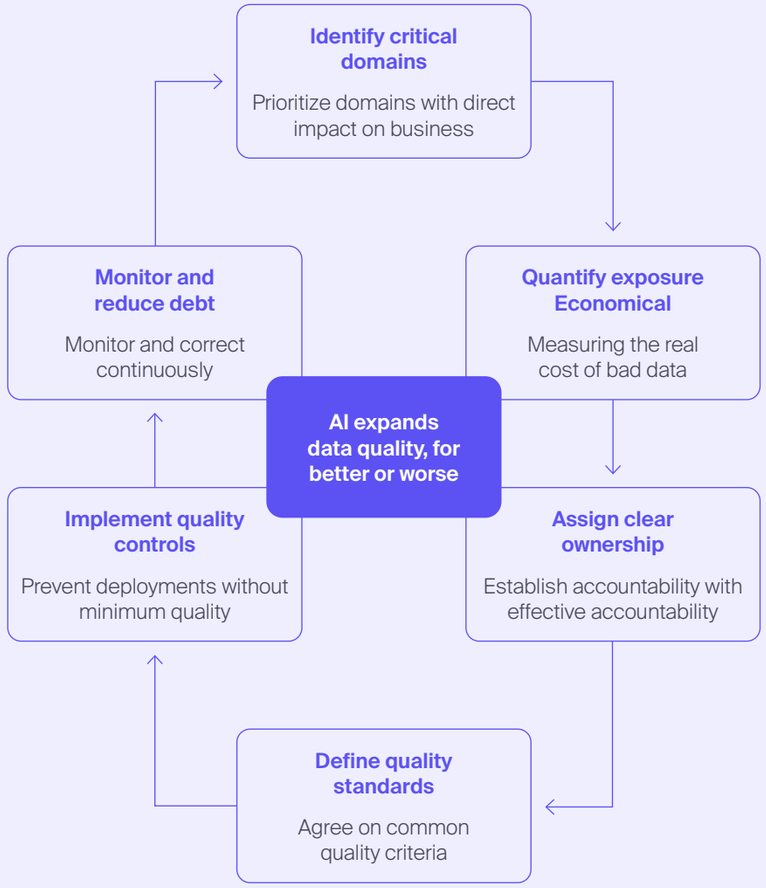
The fourth is to **introduce mechanisms that prevent the pressure to innovate from imposing itself on structural prudence**. Not every domain should feed models into production if it doesn't meet minimum standards, and incorporating quality gates before AI deployment prevents the organization from automating errors at scale.

Finally, **sanitation requires continuity**. Data debt tends to reappear as processes, systems, and priorities change. Monitoring their evolution, quantifying their impact and prioritising their reduction must be integrated into strategic planning.

Only **when data quality is managed with the same regularity as security or financial performance does it cease to be an episodic issue** and become a stable component of the operating model.

If bad data can erode a significant part of potential revenue and if the organization itself recognizes that quality is the main barrier to scaling AI, **demanding results without having cleaned up critical domains is taking unnecessary risk**.

Critical data domain sanitization cycle



Challlenge#2 | Structural Foundations | Sanitizing critical data before demanding results from AI

HOW IT IS ACHIEVED

Forcing a change in the system's incentives

To clean up critical internal data, the CIO must transform data quality into an explicit economic responsibility and a mandatory condition for operating. Today, in most companies, data lives in a gray area, where IT guards it, the business exploits it and the CFO measures financial results without direct visibility on the quality that conditions them. **This fragmentation of responsibility explains why data debt accumulates, no one is directly responsible for the economic impact of its deterioration**.

In most organizations, the business does not assume the quality of the data because it does not perceive its direct cost and IT corrects it later, then the economic impact is diluted and the urgency disappears. **As long as poor quality does not have an explicit cost for those who generate or consume the data, the organization will continue to prioritize speed over consistency**.

To meet this challenge by 2026, **the CIO must introduce a direct connection between data quality and operational performance**. This means making visible the economic impact of error in critical domains such as poorly calibrated pricing, inaccurate forecasts or faulty automated decisions, and linking it to metrics that the business already recognizes: margin, conversion, risk, compliance.

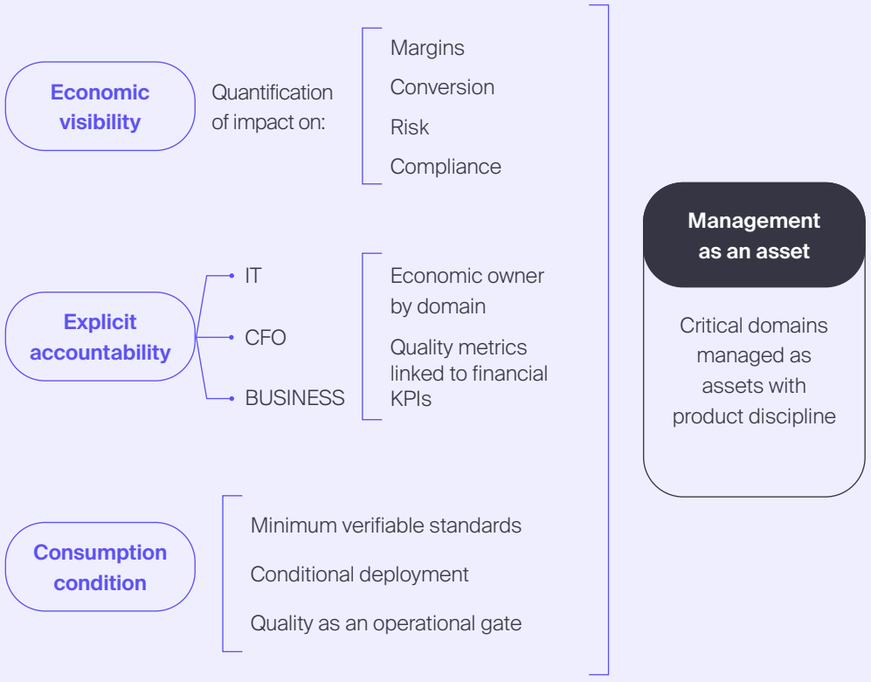
Once there is visibility, it is necessary to apply consequences. If an AI model can be deployed, even if the domain that powers it does not meet minimum standards, the system will continue to reward speed. As a CIO, **you must establish a non-negotiable operating principle, where critical domains condition the pace of deployment**. Thus, when the consumption of the data is conditioned by its quality, the organization begins to invest earlier in sanitation instead of correcting it later.

In addition, the conversation must be shifted towards exposure reduction. Instead of talking about quality in the abstract, **you have to quantify how much operational and financial risk is concentrated in each critical domain**. When the CFO understands that a significant portion of potential revenue depends on data consistency, cleanup becomes a measure of financial control.

The real change occurs when the organization internalizes that critical domains are not passive repositories, but active lifecycle repositories, and the **CIO will meet this challenge when these domains are managed with the same discipline as a product line**.

Sanitation consists, then, in **changing the rules under which data is generated, consumed and deployed**. When incentives are aligned, economic impact measured, and consumption conditioned to verifiable standards, the organization will no longer tolerate structural inconsistencies.

How to turn data quality into an economic condition



Challlenge#3 | Structural Foundations

Integrate governance, security, and observability by design

For years, organizations have operated under the premise that control can be added later. First, the focus is to build. It is then deployed or integrated, and then audited, certified, or reinforced with additional tools. **This model, inherited from perimeter architectures and linear development cycles, assumed that systems were relatively stable** and that risk could be contained in external layers.

In 2026, this premise is proven wrong. **Today's technological environments are not only more complex, they are progressively more autonomous**. Artificial intelligence is no longer limited to generating recommendations or responses, but executes actions, accesses systems, triggers processes, and makes decisions that directly impact operations and customers. Agents go from being assistants to becoming actors within the system.

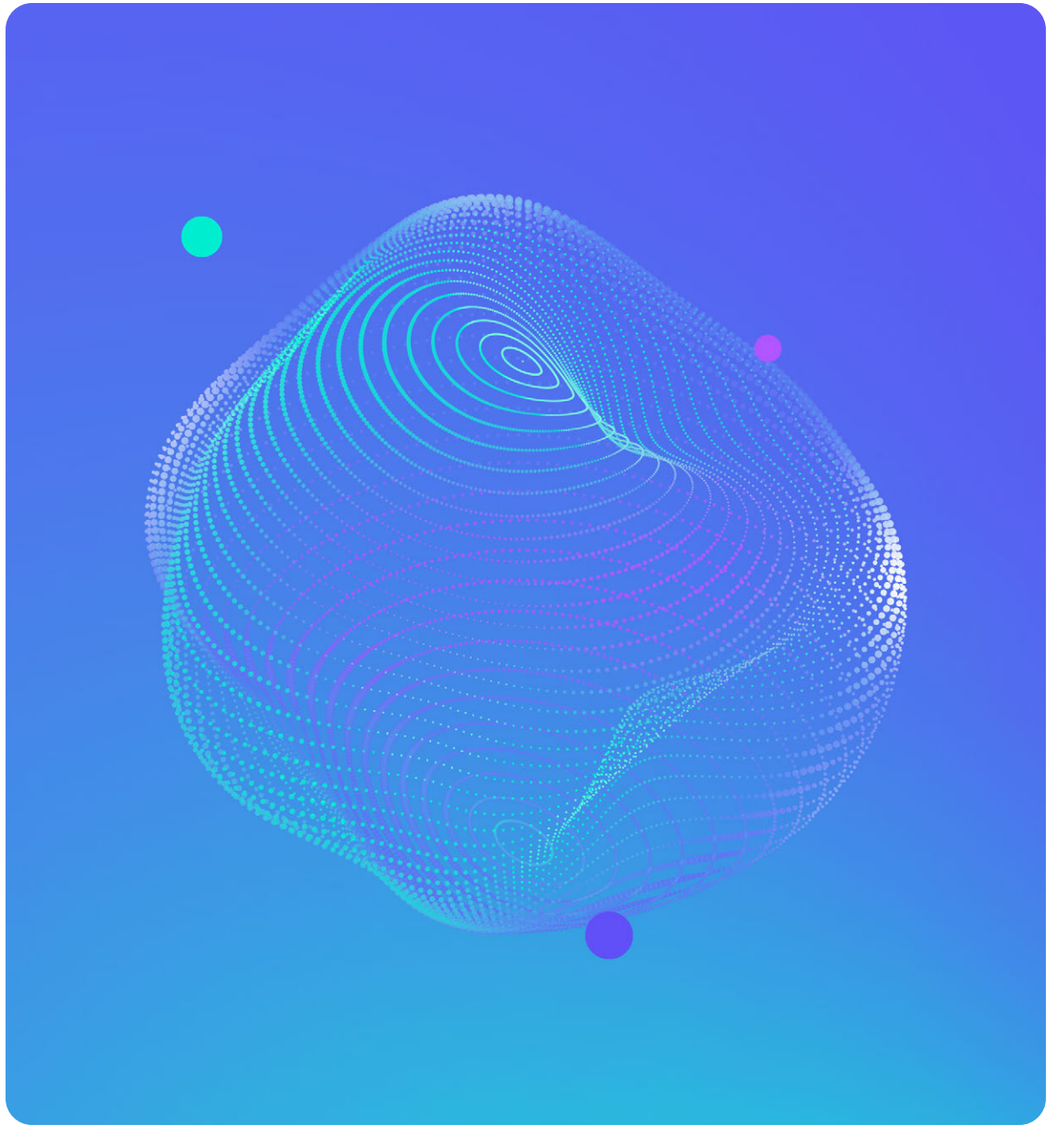
The problem now is the asymmetry between autonomy and control. **Only a minority of organizations declare that they have a mature governance model for autonomous agents, while the majority already deploy them in production**. The capacity for action grows faster than the capacity for structural supervision.

This generates a particularly delicate situation, automated decisions without full traceability, models operating without clear mechanisms for pause or reversal, and diffuse responsibilities when an agent executes an improper action. **The illusion of control is maintained as long as no visible incident occurs, but when it does, the organization finds that it cannot explain precisely what happened, under what policies, or with what data**.

Regulatory pressure is added to the gap to amplify it. **Recent regulations require explicit traceability, the ability to explain automated decisions, and reporting** in very short time windows.

This implies that the organization must not only act correctly, but also **demonstrate in a verifiable way how and under what policies an autonomous system acted**.

The problem now is that the traditional operating model is not designed for that provability. When an agent executes an improper action, modifies a sensitive configuration or generates a biased recommendation, the organization must **be able to respond and take responsibility so as not to have regulatory or even reputational problems**.



Sources: KPMG | IBM | ApproveIT | SC World | National CIO Review | zamp.ai | McKinsey

Challlenge#3 | Structural Foundations | Integrate governance, security, and observability by design

Reactive governance against risks already materialized in autonomous environments

High risk awareness, low control capacity

Risk awareness

Actual governance capacity

Only 21% of organizations **have a mature autonomous agent governance model in place**

Technological autonomy scales faster than the organizational capacity to govern it

Sources: KPMG | IBM | ApproveIT | SC World | National CIO Review | zamp.ai | McKinsey

Challlenge#3 | Structural Foundations | Integrate governance, security, and observability by design

If technological autonomy transforms the nature of risk, control can no longer operate as a parallel function. In traditional models, security and governance were organizational layers that evaluated what the system had already done. Specialized teams, regular audits, and post-deployment validations were in place. The system operated and the control then reviewed, generating a sequential and tolerant relationship.

This scheme is incompatible with environments where decisions are executed automatically and their impact is immediate. When an agent can approve transactions, modify configurations, or interact with critical systems without direct human intervention, the time between action and consequence is reduced to seconds. **In this context, any separation between design and control introduces a structural window of exposure**.

To convert control into a structural property, it is necessary to move it from the organizational periphery to the architectural core. **This means that every actionable component**, from applications, models, to autonomous agent, **must incorporate four inseparable attributes from its conception**:

Verifiable identity
No entity operates without registration, defined version and associated liability

Automatically executable policies
Preventive limit of the scope of action and non-dependence on manual interpretation

Comprehensive traceability
Record of what happened, under what rules, with what data and with what dependencies

Immediate containment capacity
Management of deviations without the need for extraordinary processes

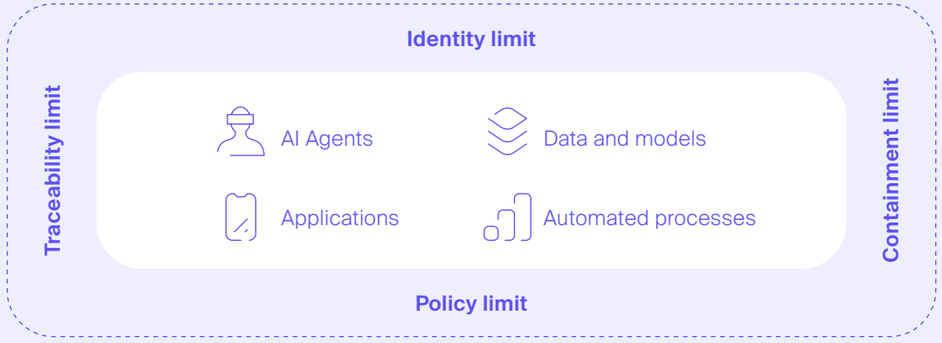
This change also alters economic logic. In the reactive model, the cost of control appears after the incident: in the form of investigation, operational disruption, and reputational impact. **In the embedded model, the cost shifts to the design, but dramatically reduces the likelihood of systemic events**.

In addition, this approach redefines the relationship with the regulator and the Council. Now, **the organization is able to demonstrate that each automated decision is inscribed in a framework of codified** policies, with traceable identity and containment mechanisms.

The logical consequence is that **governance ceases to be a function that supervises, but a property that configures**. Security is no longer applied as an additional layer and becomes the structural constraint of possible behavior, and observability is the permanent ability to understand the state of the system in real time.

Only when control is integrated in this way can the organization scale technological autonomy without multiplying invisible exposure.

Control as an architectural barrier



El sistema opera libremente, pero dentro de las barreras explícitas

Challlenge#3 | Structural Foundations | Integrate governance, security, and observability by design

HOW IT IS ACHIEVED

Redefining the technology deployment contract

Integrating governance, security, and observability by design is only achieved when **the CIO redefines the rules under which any technology, especially AI and autonomous agents, can be deployed in production**. Today, in most organizations, deployment follows a hybrid model: predominant human review, documented but not automated controls, fragmented responsibility between CIO, CISO, and business. The consequence ends up being predictable; growing autonomy with partial supervision.

The CIO achieves this challenge when he transforms deployment into a structurally conditioned mechanism. **That means no actionable model, agent, or application can go into production without meeting coded and verifiable requirements**. To do this, three structural decisions are required.

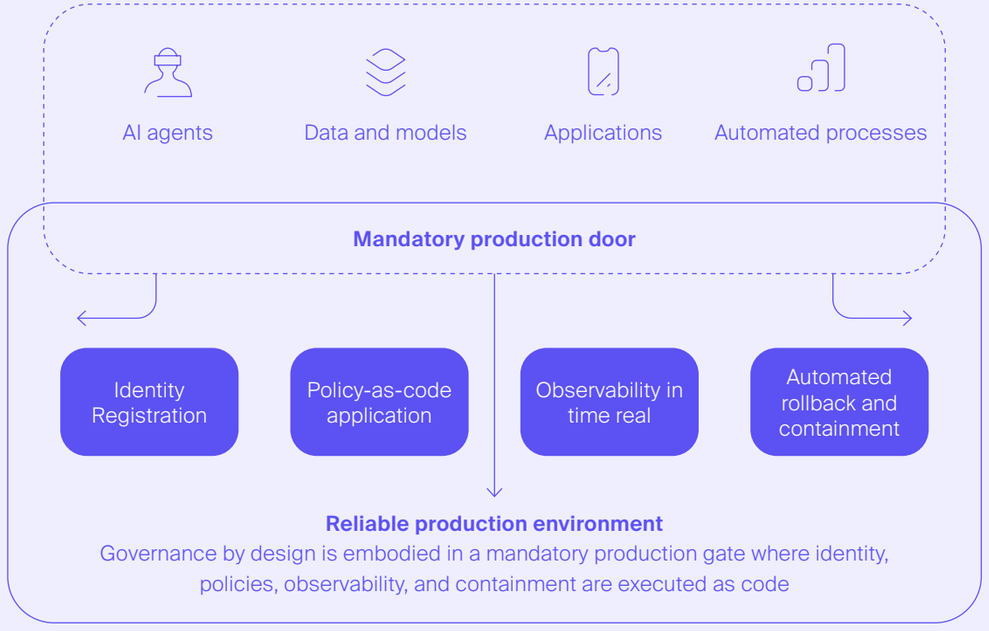
First, consolidate operational responsibility since, as long as security, architecture and data operate as parallel domains with advisory veto, control will be negotiated on a case-by-case basis. **The CIO must formalize a common mechanism**, resilience and economic impact are evaluated in an integrated manner.

Second, automate control instead of revising it. **Human review is insufficient in environments where 70% of companies already operate agents in production**. Policies must be executed as code, using mandatory identity, centralized logging, comprehensive logging, operational limits, and automated rollback capability . When control is integrated into the pipeline, autonomy is contained by design.

Third, link resilience with economic legitimacy. The average cost of a critical outage and the reputational impact of a breach are figures that the CFO and Board understand. **The CIO must translate embedded governance into tangible reduction of exposure**: lower MTTD, lower MTTR, lower probability of regulatory sanction, greater ability to explain automated decisions to audit.

This redesign also alters culture. In "move fast" environments, control is often interpreted as an obstacle. **The CIO reconfigures this tension by allowing innovation to continue to be a priority**, but operating within non-negotiable structural limits.

How governance works by design



Governed pilots become practical demonstration that speed and discipline are not incompatible. The challenge is met when the organization stops asking whether a system is sufficiently controlled after deploying it and begins to **assume that no system can be deployed if it is not born governed**.

Challlenge#4 | Scaling mechanisms

Prioritizing and financing ai as an investment portfolio

Most organizations have treated AI as a portfolio of experiments: scattered pilots, tactical use cases, and budgets approved by opportunity rather than strategy. That approach worked when the goal was to learn quickly and the cost of failure was affordable. But, **by 2026 this mindset has stopped working because AI is evaluated as a capital allocation under scrutiny**.

Evidence of scale is the breaking point; with consistently low scaling rates, pilot backlog should not be interpreted as healthy exploration, but as the **inability to convert investment into stable operational value**.

The problem is not that there is a lack of initiatives, it is that the **financing model is designed to produce activity, not return**. And when the return is uncertain, the CFO cuts AI due to a lack of economic discipline.

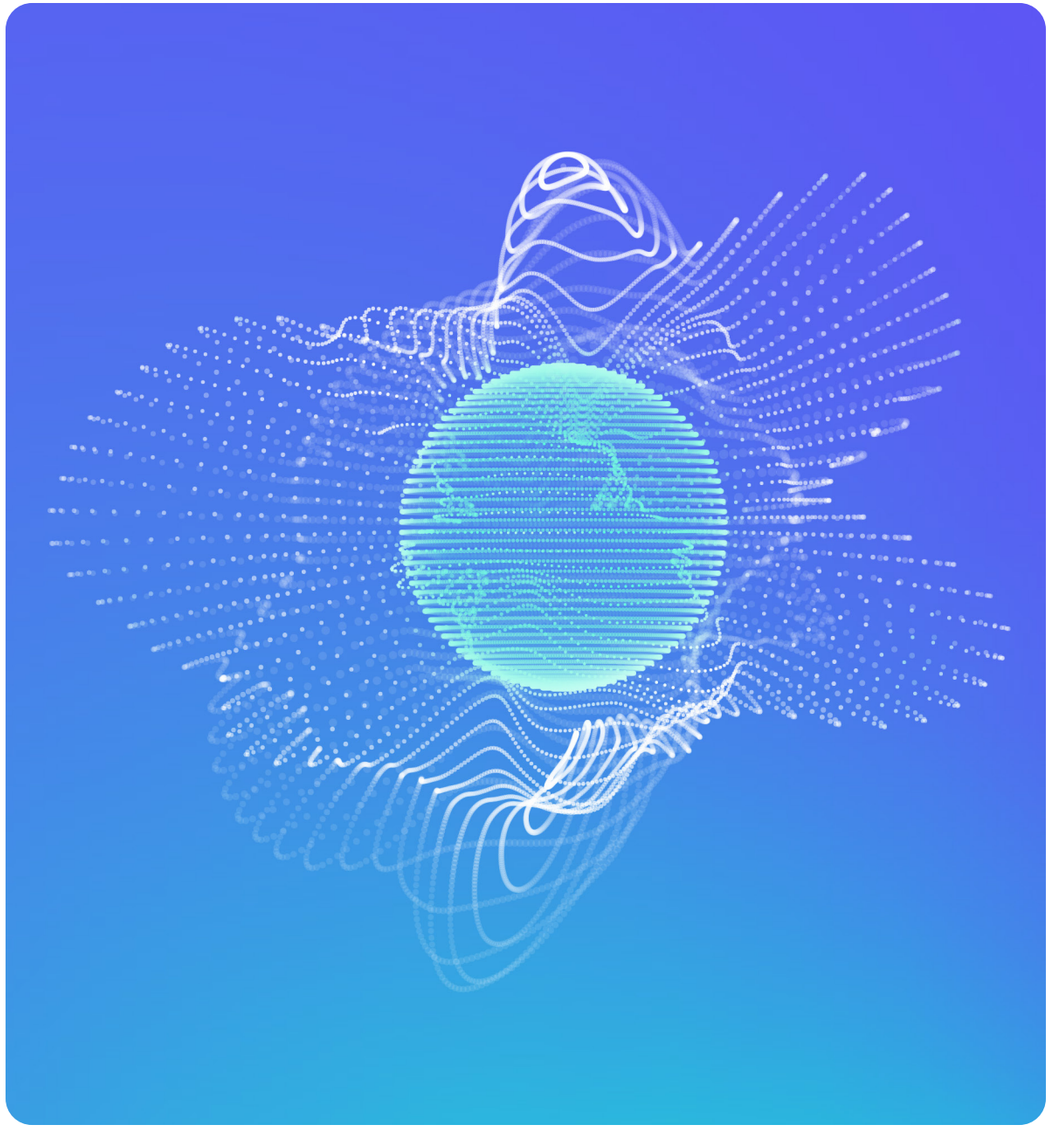
That discipline becomes inevitable for a simple reason: **AI competes against non-negotiable expenses**, such as cybersecurity development, modernization, or regulatory compliance, which absorb most of the budget, leaving AI in discretionary territory.

As long as the organization maintains a structure in which the majority of spending is dedicated to sustaining the present, any investment in AI must justify the opportunity cost of not funding resilience, compliance, or operational continuity. In this context, **AI is no longer being tested and becomes a gamble that must explain why it deserves to displace other priorities**.

The flaw of the current model is concentrated in the absence of active reassignment. In immature organizations, **initiatives without traction are prolonged by political inertia or by internal reputational fear**. This ends up wasting budget and destroying credibility.

AI ends up becoming a set of rising costs without a narrative of control and, when the market enters the "honeymoon over" **phase, the impact falls on questionable budgets, pressure for metrics and freezing of initiatives that cannot demonstrate accumulated value**.

The challenge, therefore, is to move from a regime of experimentation to a regime of capital, where **the organization knows what it finances, why it does it, what evidence it needs to continue and what it is willing to cancel to free up resources**.

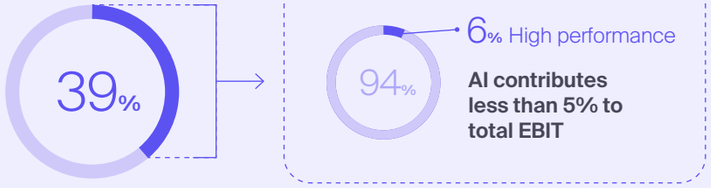


Sources: Info Tech | McKinsey | II | III | The CFO | AMS | CFO | Open AI | Demócrata | State Tech

Financial impact of AI at the enterprise level

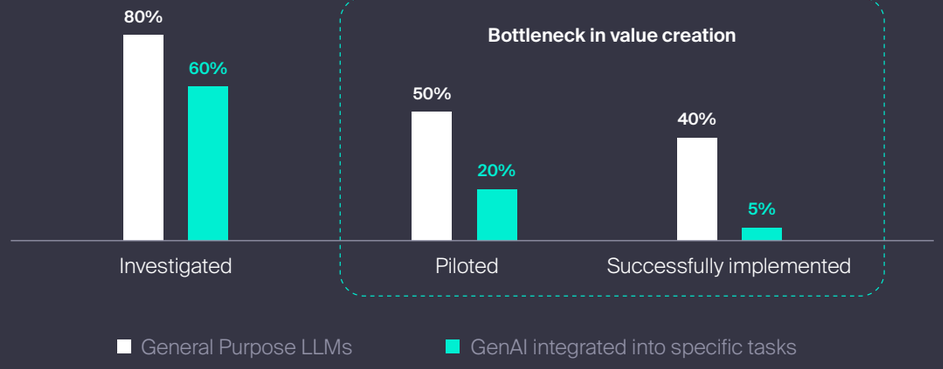
% of companies worldwide

Companies attributing some level of EBIT impact to AI



Despite the proliferation of initiatives, most organizations have failed to translate AI into material financial impact, straining their budget sustainability

The gap in GenAI: adoption vs implementation



Sources: Info Tech | McKinsey | II | III | The CFO | AMS | CFO | Open AI | Demócrata | State Tech

Challlenge#4 | Scaling mechanisms | Prioritizing and financing ai as an investment portfolio

If the problem is not a lack of use cases, but the inability to turn them into structural financial impact, then the solution cannot be limited to making better pilots. The change required is more profound, **AI must now be managed as a capital architecture, rather than as a collection of technology initiatives**.

In the current model, each use case competes for budget in isolation. A business case is presented, a pilot is approved, a limited set of operational metrics is measured, and if the project does not generate immediate rejection, it is maintained. **This logic produces dispersion and multiple initiatives advance in parallel without a clear hierarchy** of strategic impact.

The portfolio paradigm alters the unity of decision. The question is no longer about the interest of each use case, and begins to revolve **around which value streams you want to concentrate capital and organizational capacity**.

AI **is prioritized for its ability to eliminate friction in critical value chains**, introducing focus where previously there was only perceived and unfounded enthusiasm.

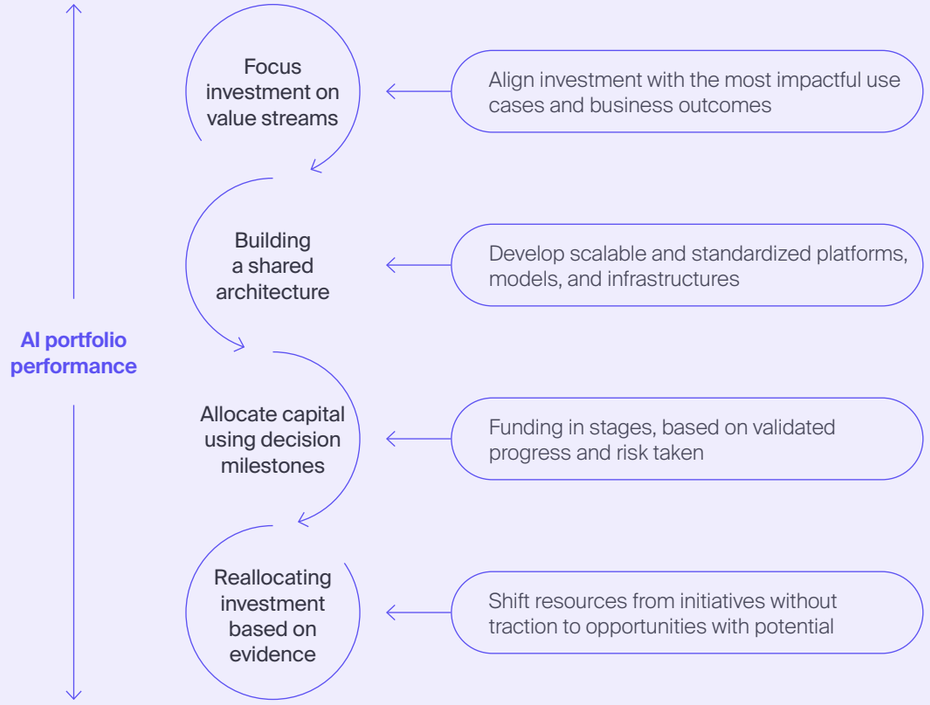
The strategic focus is insufficient without architectural leverage, so **organizations that do not share infrastructure, data, and evaluation mechanisms turn each pilot into an island**. Each island has its own marginal cost, its own technical debt, and its own supplier.

Enterprise architecture also becomes the economic multiplier of the portfolio, with common data, reusable models, standardized evaluation layers, and shared platforms reducing the cost of scaling and increasing return comparability.

The third component is equity discipline. Capital is allocated incrementally, conditional on accumulated evidence. **Active cancellation**, specifically that 42% of initiatives without ROI that mature organizations are willing to stop, is a **sign of financial maturity**.

The reallocation from low-yielding initiatives to bets with real traction is what transforms AI from uncertain spending to governed investment.

Capital conversion cycle to AI



This approach ends up redefining internal politics, **when artificial intelligence is financed as a strategic portfolio, the company decides its bets and defends them collectively**. The difference between activity and competitive advantage lies here. Those who manage AI as a sum of use cases accumulate initiatives, those who manage it as a capital architecture accumulate strategic capabilities that alter the economics of the business.

Challlenge#4 | Scaling mechanisms | Prioritizing and financing ai as an investment portfolio

HOW IT IS ACHIEVED

Installing an institutional ai investment regime

The CIO meets this challenge when **he integrates AI into the company's ordinary capital allocation regime and establishes explicit financing, monitoring, and exit rules for each initiative**. In this way, AI is subject to the same economic, strategic and risk criteria as any other relevant technological investment.

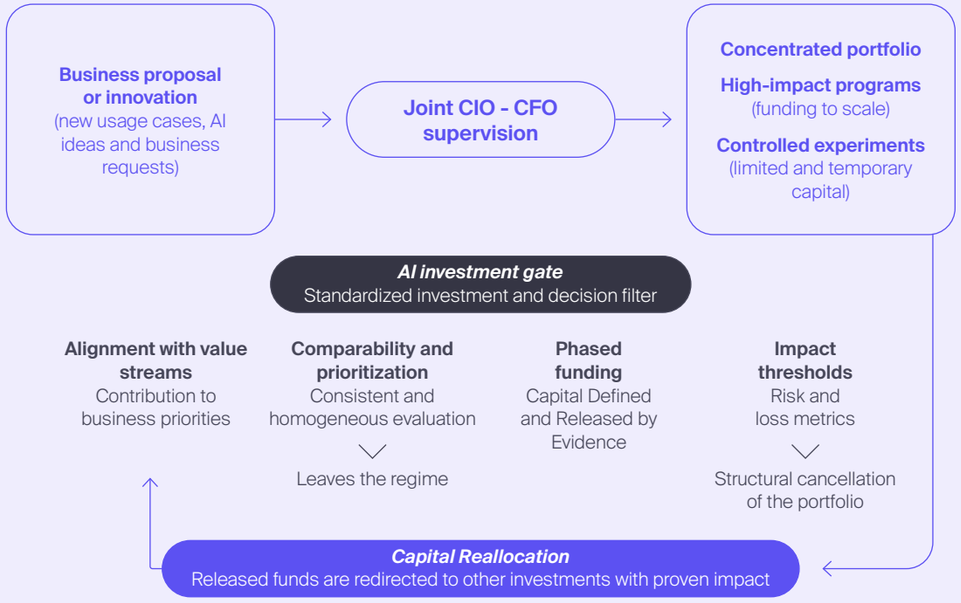
First, it is advisable for the organization **to define a mandatory evaluation framework that classifies each initiative according to its contribution to priority value streams, its scalability potential, and its exposure to risk** and regulatory compliance. These criteria determine the volume of capital allocated, the pace of investment and the conditions of permanence in the portfolio, allowing real comparability between initiatives and avoiding decisions based solely on technological attractiveness.

The model also incorporates a formal system of stages with defined quantitative thresholds, so that each phase requires cumulative evidence of economic impact, operational adoption, and technical feasibility. **Funding continues when indicators reach established levels and is interrupted when traction is insufficient**, consolidating cancellation as a structural and not an exceptional practice. Consequently, this mechanism disciplines capital and prevents the accumulation of projects sustained by inertia.

In addition, **the CFO participates as a co-owner of the AI portfolio and validates, together with the CIO, the decisions of continuity, scaling and closure** in the same committees that review the rest of the strategic investments. This shared oversight strengthens financial coherence, reinforces legitimacy before the Board, and turns the conversation into a systematic analysis of return, risk, and concentration of resources.

The savings generated by efficiency and by the cancellation of initiatives without traction are redirected towards **programs with demonstrated impact on margin, productivity or structural risk mitigation**, and the flow of capital is documented and explicitly linked to measurable results, which allows demonstrating progression and justifying budget increases when the evidence supports it.

How to integrate an AI investment regime



In this way, a process is generated where AI is manageable as disciplined capital

In this order, AI is fully integrated into regular budget planning and review cycles, consolidating governance as a stable practice and reducing ad hoc funding. The portfolio **evolves with consistent criteria and maintains a focus on strategic bets supported by shared architecture and homogeneous metrics**.

The result is a **concentrated, disciplined and transparent investment system, capable of raising the rate of scaling and increasing the financial contribution of AI** through strategic focus, comparability and structural reallocation of capital.

Challlenge#5 | Scaling mechanisms

Turning rapid innovation into scalable products

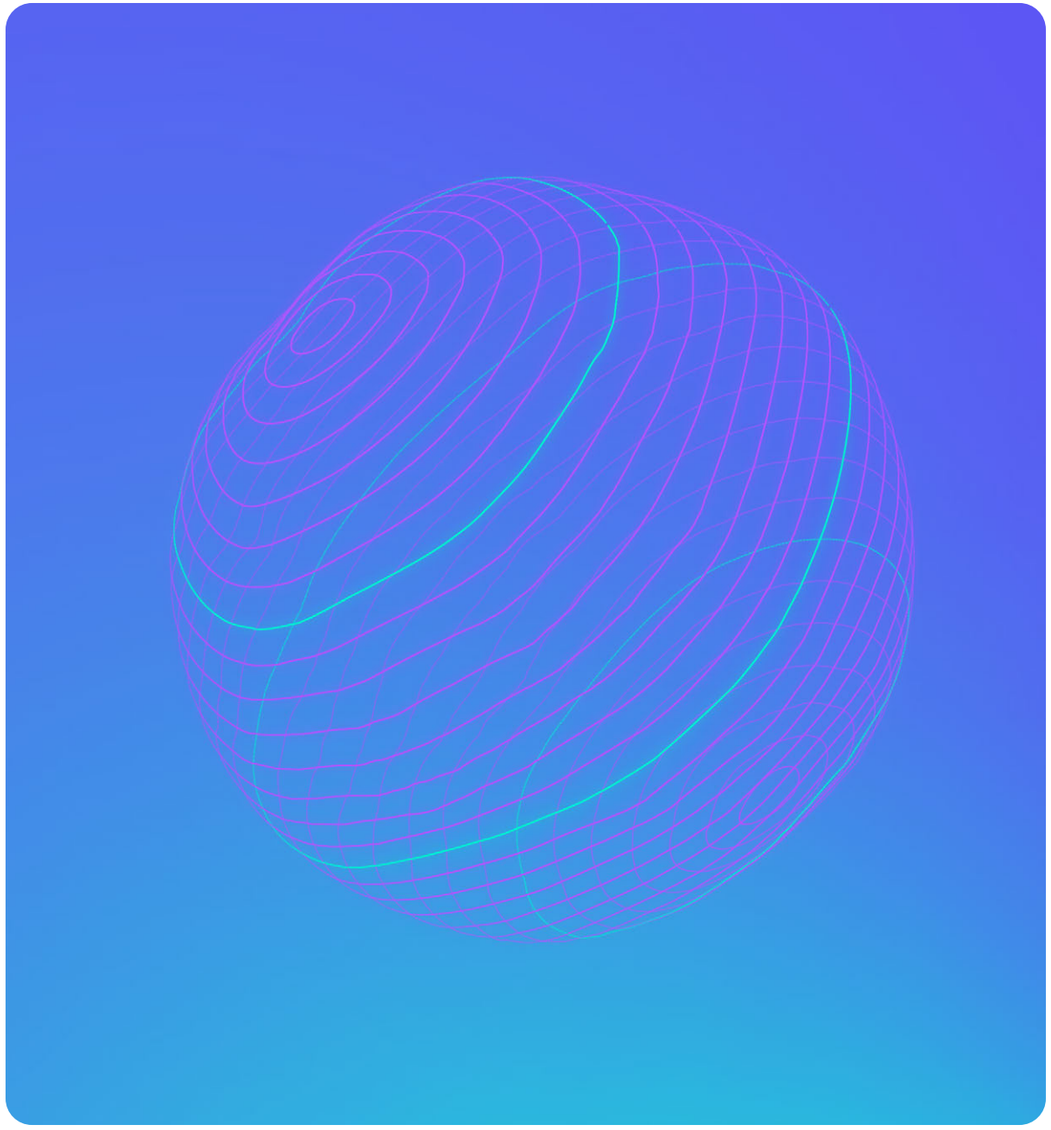
As already pointed out in the previous challenge, investment discipline is essential to avoid the dispersion of capital in initiatives with no return. However, even in organizations that have begun to govern AI as a portfolio, **a large majority of initiatives do not achieve stable production or generate sustained value**.

The pattern tends to repeat itself; the pilot validates a technical hypothesis, arouses initial interest and consumes specialized resources, but stalls before being integrated into critical processes. **When the transition to production exceeds certain time thresholds, the likelihood of significant impact is drastically reduced and executive momentum is diluted**. The initiative then remains active without scaling or is canceled without having built reusable capacity.

Economic magnitude is essential in this area. Each stalled pilot absorbs capital, talent, and managerial attention, and can account for hundreds of thousands or millions in investment with no operating return. On an aggregate scale, **the accumulation of non-industrialized experiments generates a significant structural cost and erodes internal confidence in the organization's ability to turn innovation** into results.

The friction is particularly concentrated in the current operating model, where many initiatives lack clear ownership, stable teams, evolutionary backlog and architecture ready to scale. And, therefore, **experimentation advances faster than institutionalization**.

In addition, accelerated innovation introduces measurable technical debt and a substantial part of the development time can be spent on rework, accumulated complexity or adjustments derived from decisions made under speed pressure. **This debt limits future capacity and raises the marginal cost of each additional deployment**. The result is an environment where the organization demonstrates creativity and experimentation, but **does not consolidate products integrated into the core business**.

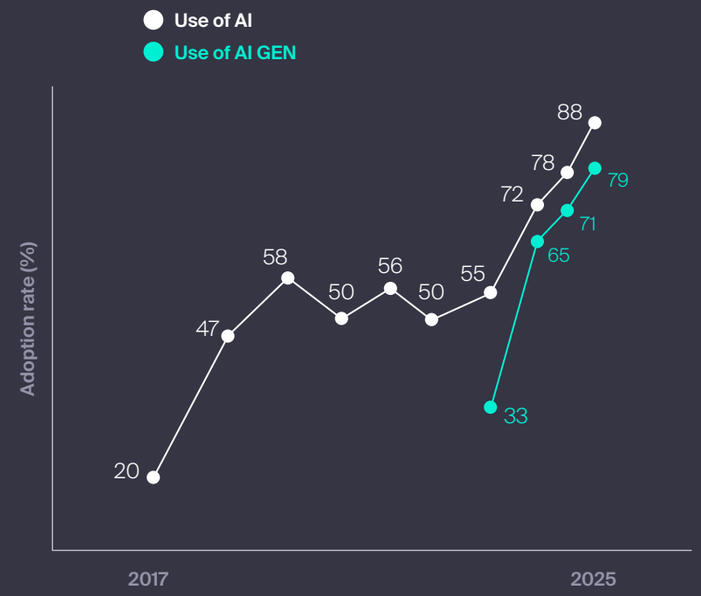


Sources: Fortune | Bain & Company | KPMG | Unframe | The CAIO Hub | CIO | AI Governance Group | Forbes | Beam.Ai | McKinsey

Challlenge#5 | Scaling mechanisms | Turning rapid innovation into scalable products

Adopting AI against the industrialization gap

AI adoption
Global growth in AI adoption (2017–2025)



AI Maturity
Organizational Maturity Distribution in AI (2025)

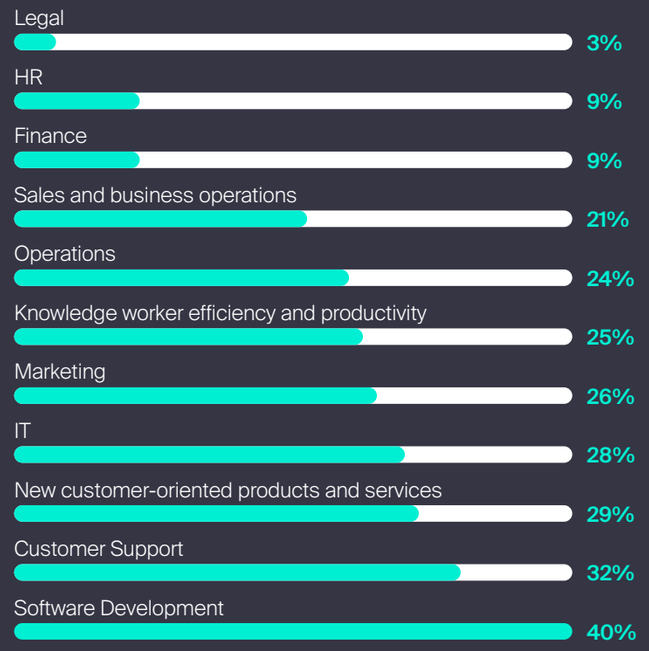
Lined-up:
Fully developed and integrated AI

In scaling:
Increasing the development/ adoption of AI

Pilot:
Testing different AI use cases

Experimentation:
any AI test

Scaling use cases by domain
%



AI adoption continues to grow rapidly, but consolidation into full production remains limited and uneven

Sources: Fortune | Bain & Company | KPMG | Unframe | The CAIO Hub | CIO | AI Governance Group | Forbes | Beam.Ai | McKinsey

Challlenge#5 | Scaling mechanisms | Turning rapid innovation into scalable products

The ability to experiment quickly has been established in many organizations; validations occur in weeks, models are tested with great agility, and teams generate functional prototypes at relatively low marginal cost. However, **while this initial velocity creates knowledge, competitive advantage arises only when that knowledge is converted into an operational asset** embedded in critical processes.

The change in logic requires treating each initiative with potential as a product from an early stage. This involves **assigning explicit responsibility for its evolution, defining real adoption metrics and establishing a continuous backlog** aimed at incremental improvement. In this way, the initiative is no longer dependent on a temporary team and is supported by a stable structure that manages performance, quality and growth over time. The objective is that operational continuity becomes a condition of scalability.

Enterprise architecture takes on a structural role in this transition, through the systematic reuse of components, standardization of platforms and modularity, reducing the accumulated friction between pilot and production. Organizations that **consolidate a common infrastructure achieve substantial reductions in portfolio costs and significantly shorten deployment cycles.**

Explicit and conscious management of technical debt completes the system: accelerated innovation introduces cumulative complexity, fragile dependencies, and tactical decisions that, while allowing for initial rapid progress, increase the marginal cost of each new iteration. **This complexity ends up being transferred to the future in the form of rework, intensive maintenance and limitations to scale**.

When the organization systematically measures the innovation and scalability process, it transforms an invisible friction into a manageable variable. Industrialization **requires this permanent visibility and sustained discipline to reduce complexity** before it compromises productive capacity.

Likewise, integration into the core business requires **standards equivalent to those of any critical system**: reliability, security, observability and governance. This ensures that the pilot product is conceived as a structural component of the operating model, with clear availability and performance requirements. Therefore, **scale is not added later, but is designed as an inherent attribute**.

Industrialized innovation system

Effective productization depends on establishing clear ownership, stable teams, shared architecture, and integrated deployment

Challlenge#5 | Scaling mechanisms | Turning rapid innovation into scalable products

HOW IT IS ACHIEVED

Redefining the technology deployment contract

The CIO can take responsibility for this challenge by generating a contract that turns the transition from pilot to product into an institutional decision, supported by enterprise architecture and connected to real delivery cycles. The starting point is **to define the contract as a cross-cutting operational policy, with explicit scope on any experimental initiative intended for deployment**, and with shared business sponsorship to ensure that the deployment is perceived as an operational commitment and not as an exploratory activity.

The first condition is **to create a single admission and scaling forum that acts as a deployment authority**. The CIO integrates it with architecture, operations, security, and business leaders, and mandates it to accept, reject, or sandbox pilots. This forum does not seek to be a bureaucratic committee, but to function as an instrument of coherence, where it is decided what enters the real delivery cycle and what remains in exploration, protects productive capacity and prevents the organization from multiplying parallel solutions.

The CIO then **formalizes the contract criteria as reusable deployment rules**. The organization defines a brief set of conditions that every initiative must meet to be consolidated as a product: formal responsibility of the owner, team assigned for the life cycle, integration with common architecture, minimum support and operability requirements, and sufficient evidence of real use or need. These criteria are published as a corporate standard, incorporated into the architecture catalog and applied consistently, which reduces arbitrariness and accelerates decisions.

The contract is made enforceable by integrating it into the actual delivery flow. First, **by eliminating the parallel prototyping circuit and taking the experimentation to the same pipeline as the rest of the product**, with guardrails proportional to the level of maturity.

Enterprise architecture supports the contract with a pillar of reusable components. The **CIO drives a catalog of deployment patterns and templates that shorten the cycle and prevent reinvention**. Reuse becomes an operational condition and the architecture team takes an active role in the design of pilots with a productive vocation to preserve coherence.

The contract is consolidated when the CIO reinforces it with incentives and adoption governance, so **teams are given autonomy to experiment, and assume obligations** when they apply for entry into production. The business participates as a co-owner of the deployment by assigning owner and committing adoption, which reduces the usual pattern of pilots without real integration.

With the contract in place, the organization **maintains the speed of innovation and builds scalable products with technical and operational continuity**.

How to implement a deployment contract

- **Mandate and authority**
  - Define contract as a corporate deployment policy that establishes IT-business authority and sponsorship
- **Governance instrument**
  - Implement admission criteria that determine which initiatives enter and at what stage
- **Embedded Delivery Integration**
  - Require every initiative with a vocation for deployment to use proportional deliveries and pipelines
- **Architectural backbone**
  - Sustain the contract on shared platforms, reusable patterns and standards
- **Sustainability discipline**
  - Condition the entry into production to compliance with minimum metrics

Challlenge#6 | Scaling mechanisms

Redesigning the talent model for human-AI collaboration

Automation is already transforming work content, and a substantial portion of repetitive cognitive tasks such as reporting, preliminary analysis, routine validations, basic reconciliations, operational documentation, can **be executed by AI systems with greater speed and consistency than traditional manual processes**.

However, organizational architecture remains anchored in structures designed to maximize direct human execution. This gap generates a constant tension that rubs against the current reality. **Organizations incorporate AI tools, but maintain roles defined by tasks that tend to be automated**.

Therefore, the consequences are reflected in inefficient overlap, that is, **people continue to execute delegable activities while trying to monitor results generated by systems**, which increases cognitive load instead of reducing it.

We can see the mismatch of this situation reflected in **three organizational dimensions**:

Dimensions of human-AI mismatches

Organizational culture

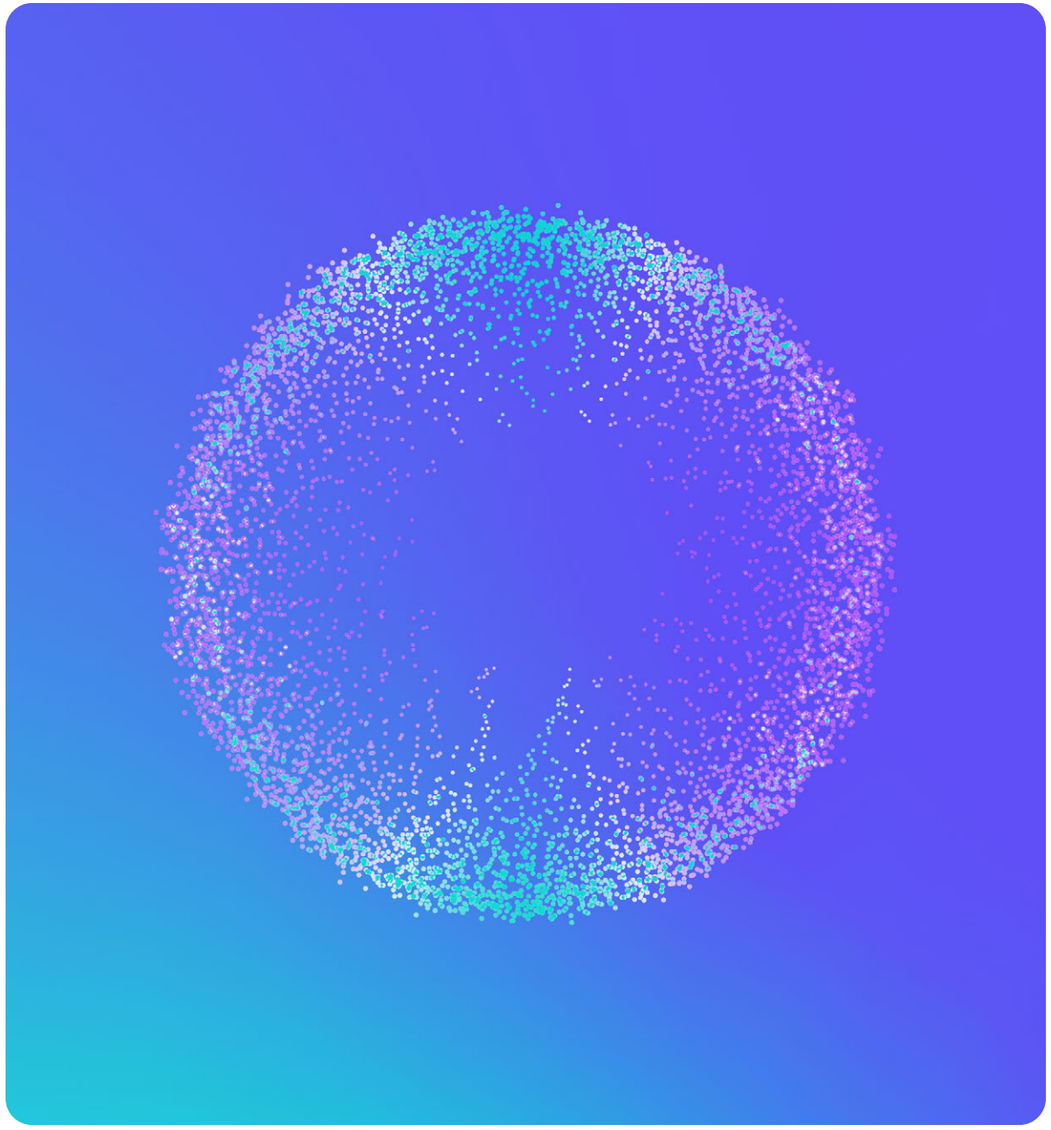
Teams incorporate AI without redefining responsibilities, reducing **consistency and scalability**

Productivity

The potential doesn't translate into performance because **workflows aren't redesigned** to integrate automated execution

Capabilities

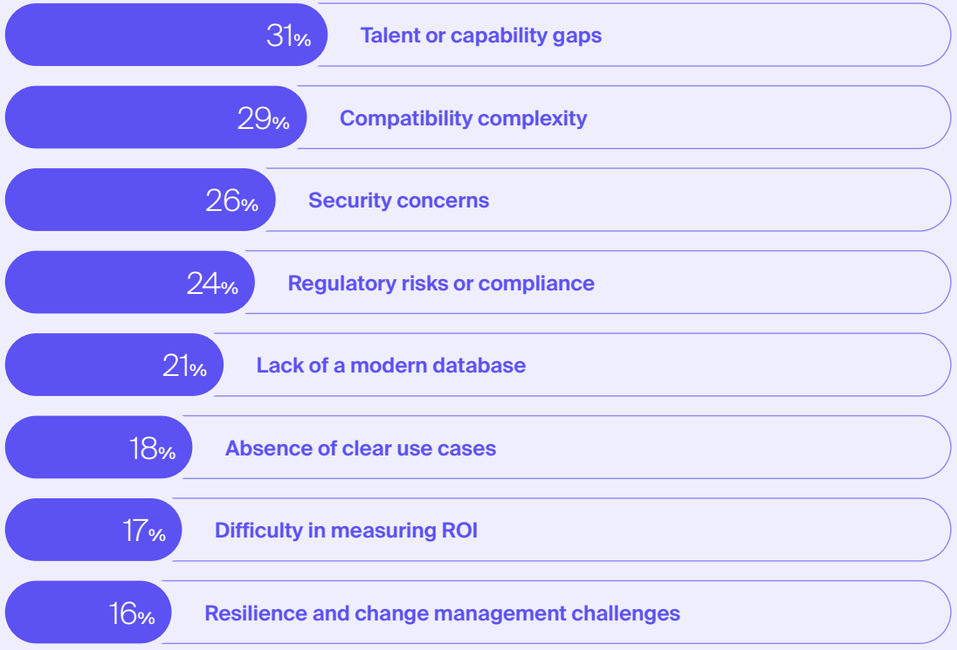
The market reflects **a shortage of skills in monitoring, interpreting, and orchestrating** automated systems



Sources: CIO | The CAIO Hub | McKinsey | II | III | Mindbreeze | IDC

Challlenge#6 | Scaling mechanisms | Redesigning the talent model for human-AI collaboration

Top challenges in ai adoption (%)



Technology is poised to amplify human capacity, but the organizational structure has not evolved at the same pace. Without deliberate redesign of roles, teams, and performance metrics, the organization introduces automation without transforming its work model, and **the potential for human-AI collaboration is limited to marginal improvements**.

Sources: CIO | The CAIO Hub | McKinsey | II | III | Mindbreeze | IDC

Challlenge#6 | Scaling mechanisms | Redesigning the talent model for human-AI collaboration

Collaboration between people and AI systems does not emerge spontaneously due to the mere availability of technology, it requires **redesigning the talent model so that the interaction between human judgment and automated execution** is coherent, stable and value-oriented.

The redesign begins with productivity, which is no longer measured by the volume of tasks executed individually and is redefined as the ability to effectively orchestrate between people and intelligent systems. This redefinition alters the role architecture, and **functions are reconfigured towards monitoring, validation, flow design, decision-making, and continuous improvement**. Repetitive execution loses centrality and responsibility for the result gains weight.

The second change affects capabilities. The CIO cannot solve the mismatch by hiring specialized profiles in isolation, **the talent problem is solved through a structured program of upskilling and internal mobility**. The organization must identify which tasks are automated, which responsibilities evolve, and which competencies become critical in the new environment. AI literacy is integrated as a transversal competence, not as a specialization limited to a small team.

Hand in hand, the logic of the team structure must also change. Traditional models organized by fragmented roles or tasks do not maximize the value of human-AI collaboration. **The organization evolves towards teams oriented towards product and business results, where domain knowledge, technological capacity and operational responsibility coexist**. Workforce transformation is closely linked to the consolidation of product-oriented leaders, capable of integrating technology and value in the same management unit.

The change in logic also seeks to reduce dependence on "star" profiles. In a hybrid environment, competitive advantage should not revolve around isolated individuals with advanced technical knowledge, but rather around a **broad base of professionals capable of interacting effectively with automated systems**. AI scaling depends on both talent and technology, which forces you to distribute capabilities and avoid excessive concentrations of critical knowledge.

The resulting hybrid model combines explicit human accountability, integrated automation, and value-driven teams. **The organization maintains strategic control, amplifies capacity through AI, and builds resilience by distributing competencies across the board**.

From individual performance to human-AI orchestration

Challlenge#6 | Scaling mechanisms | Redesigning the talent model for human-AI collaboration

HOW IT IS ACHIEVED

Institutionalizing a hybrid human-ai work model

Talent redesign is installed as a **transversal organizational policy, with shared leadership between CIO and CHRO and with explicit impact on structure, roles and performance metrics**. Technology defines the new operating environment, while human resources translates that reality into capability architecture. In this way, both act as co-architects of the work model.

To meet this challenge, the first move is to **formally declare the transition to a hybrid model as a strategic priority, linking it to productivity, resilience and scalability of AI**. This statement enables the systematic review of existing roles. The CIO, together with business and HR leaders, drives structured task mapping, identifies where automation is already viable, and determines which responsibilities evolve into oversight, flow design, validation, and continuous improvement.

Subsequently, a modular governance of talent is established. Instead of an abrupt transformation, **the organization moves by domains or units, applying the same redesign framework in each module**.

This controlled progression allows learning to be adjusted, practices to be consolidated and cultural friction to be reduced. In each of the modules, three clear decisions are incorporated: **which tasks are automated, which skills are developed and which roles are reconverted**.

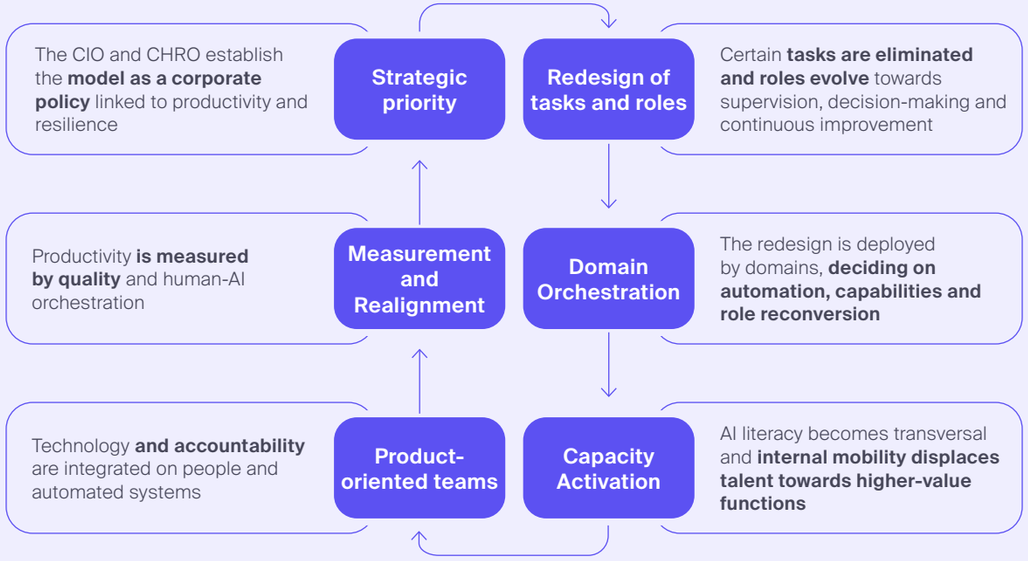
The third movement articulates reskilling as a gradual and incremental mechanism. **Progressive upskilling ensures that AI literacy becomes a** core transversal competence. At the same time, **internal mobility is institutionalized as a strategic tool**, facilitating the transition from repetitive tasks to functions with greater added value.

As a result, teams are reorganized around product and value. The CIO **drives the transition from purely functional structures to stable units that integrate domain knowledge, technological capabilities, and operational accountabilit**y. These teams manage both people and automated systems within a single accountability framework.

The CIO's fifth move is about **redefining organizational metrics, where productivity is evaluated by quality of output, orchestration capacity, and continuous improvement supported by automation**. Individual and collective performance incorporates criteria linked to collaboration with intelligent systems, continuous learning and contribution to business value.

When these movements are installed in a coherent and progressive way, the organization evolves towards a sustainable hybrid model. **Technology amplifies human capacity, roles reflect operational reality, and organizational structure supports collaboration with intelligent systems** as a constituent part of work.

Cycle of institutionalization of work



Challlenge#7 | Strategic legitimacy

Demonstrate business impact and credibility to the C-level

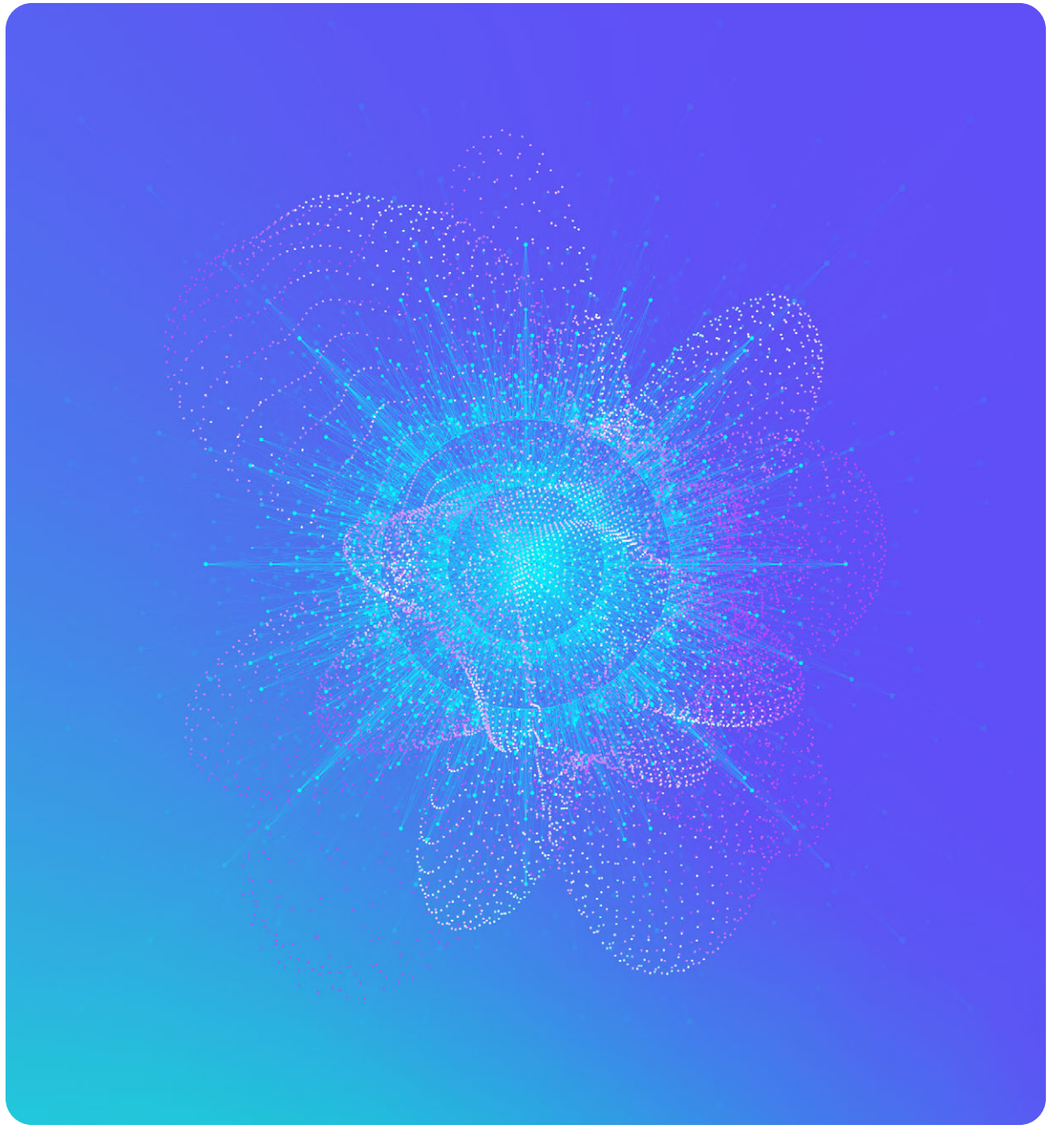
The latest tension facing the CIO in 2026 is not operational, it is strategic. **There is a persistent gap between the outcomes that IT measures and the outcomes that the C-level** needs to validate. And, while the technology function reports stability, deployment of tools and operational efficiency, the CEO and the Board demand clarity on margin, growth, return and risk exposure.

The friction is particularly evident around the development and implementation of AI. After an initial phase of enthusiasm, **the executive committees have raised the bar on demand**. The lack of scaling of pilots and their disconnect in the P&L link is evident and the discourse on adoption and experimentation has lost steam because it does not translate into tangible economic impact.

Added to this tension is the fragmentation in the narrative of risk and capital: the CIO reports availability and modernization, the CISO incidents, the CFO reports spending. But, without clear integration, technology appears as a sum of activities, not as an architecture of business resilience. **The absence of a unified framework makes it difficult to demonstrate how ecosystem simplification, governance by design, or investment discipline reduce exposure and strengthen strategic stability**.

In addition, there is a **clear confusion between the priorities of the CEO and the needs of the CIOs**, which leads to distrust to influence long-term strategic decisions. The internal optimism about budget growth contrasts with the caution of the rest of the committee and this divergence reveals a division of expectations where, on the one hand, the CIO talks about technological capabilities and, on the other, the CEO listens in terms of business results.

Now, the organization seeks to validate the evidence of impact. The CIO can consolidate his position when he connects each initiative with business indicators and metrics, prioritizes with economic criteria and abandons projects without visible traction. **After simplifying, governing, prioritizing, industrializing, and redesigning talent, the CIO must demonstrate that those decisions have modified the economic and competitive structure of the company**.



Sources: McKinsey | II | III | IV | V | Gartner | CIO | Netskope | PwC

Challenge#7 | Strategic legitimacy | Demonstrate business impact and credibility to the C-level

Engagement without mandate: the friction between CIO and CEO

The data show that the CIO is present in the strategic conversation;

But that conversation continues to be validated with metrics that it does not lead

By performance

By technology spend (2025 tech spend)

% who say CIOs are actively involved in developing business strategy

of **CIOs aren't sure they understand what their CEO really wants**

do not feel empowered to make long-term strategic decisions

Sources: McKinsey | II | III | IV | V | Gartner | CIO | Netskope | PwC

Challlenge#7 | Strategic legitimacy | Demonstrate business impact and credibility to the C-level

The CIO consolidating his position in 2026 understands that the problem is not the lack of metrics, **but the disconnect between what is measured and what the committee considers strategic**. For years, the technology function has reported stability, efficiency and deployment of capabilities, however, the Board does not deliberate in terms of uptime, it deliberates in terms of margin, growth, risk and capital allocation.

The necessary change in the future consists of **moving the conversation from technological execution to the economic and strategic transformation that this execution produces**. In today's environment, enthusiasm for AI has given way to scrutiny.

When the CIO connects every initiative and decision made to structural productivity, sustainable efficiency, or new revenue streams, the conversation moves forward. The same goes for risk, the organization may exhibit high levels of availability, but the committee **wants to understand how technology architecture reduces regulatory exposure, mitigates reputational risk, and strengthens resilience** in the face of disruptions.

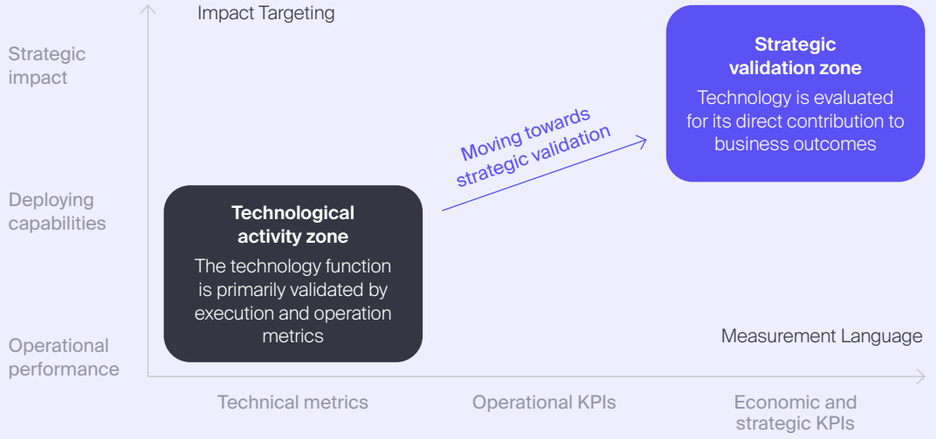
The traditional fragmentation between the different figures of the C-level loses effectiveness in a context where technological risk is business risk, therefore, **the new logic must integrate these dimensions into a single strategic story**.

Reported support from business partners

44	Business partners support long-term investment in platforms
35	They are willing to invest in risk mitigation
25	Actively participate in the planning and prioritization of initiatives
16	Are effective in defining requirements
13	They invest in changing ways of working

The CIO receives occasional support from the business, but rarely sustained co-responsibility throughout the decision cycle

Shift to strategic validation



In terms of capital discipline, prioritization and abandonment become signs of strategic focus. **The CIO demonstrates maturity when he links technology investment to explicit decisions about the allocation of scarce resources**.

This shift in logic requires clarity on what really matters to the CEO. With strategic validation, the CIO is forced to **understand which conversations are critical, what metrics sustain those conversations, and how to structure the dialogue** to facilitate optimal decision-making.

Thus, simplification translates into capital liberation and reduction of complexities, governance integrated into resilience, AI management as a portfolio in value scalability, standardized innovation is validated by real adoption and economic contribution and hybrid talent is reflected in expanded productivity.

As a result, **the CIO stops championing initiatives and begins to validate strategic outcomes**, and technology is integrated into the core of business decision-making.

Sources: McKinsey | II | III | IV | V | Gartner | CIO | Netskope | PwC | KPMG

Challlenge#7 | Strategic legitimacy | Demonstrate business impact and credibility to the C-level

HOW IT IS ACHIEVED

Reconnecting technology, value and decision in the committee

The CIO consolidates strategic credibility when **they turn technology into a recurring and verifiable business conversation within the executive committee**. This reconnection occurs through the deliberate redesign of the measurement, decision, and prioritization framework.

The first step is **to link each relevant technology initiative to one or more explicit business KPIs**. In this way, projects are not approved for technical sophistication or innovative pressure, but for their direct contribution to margin, growth, resilience or structural productivity. It is crucial to establish a discipline where no strategic initiative reaches the committee without a clear and understandable economic translation.

The second move involves redesigning the AI and automation metrics system. The CIO **incorporates indicators that capture indirect value, cumulative impact and structural improvement**, beyond immediate efficiencies. Validation includes risk reduction, acceleration of operational flow, liberation of human capital and improvement in decision-making quality. In addition, these metrics should be reviewed periodically with the same intensity with which other strategic investments are evaluated.

The third element is the visible discipline of prioritization and abandonment. Consolidating credibility when **you turn technology prioritization into an explicit economic conversation within the committee**. It presents comparable scenarios, exposes trade-offs, and links investment or reallocation decisions to tangible financial impact.

The fourth move is to integrate technology, risk, and capital into a unified narrative alongside the CFO and CISO. The CIO actively participates in the **construction of a strategic scorecard** where simplification, governance, talent and portfolio are expressed as exposure reduction, structural stability and competitive scalability.

The fifth element is to raise the level of conversations with the CEO. **Identifying which issues are critical for strategic direction and structuring the dialogue** around those priorities, thus reducing the gap in expectations between both figures and positioning the CIO as a strategic interlocutor.

When these movements are consolidated, strategic validation becomes institutional practice. This is the natural closure: **prioritizing, simplifying, governing, industrializing and redesigning talent makes full sense when it allows us to demonstrate how technology redefines the economic and competitive structure** of the company.

How to reconnect technology to business value

Softtek®

softtek.com