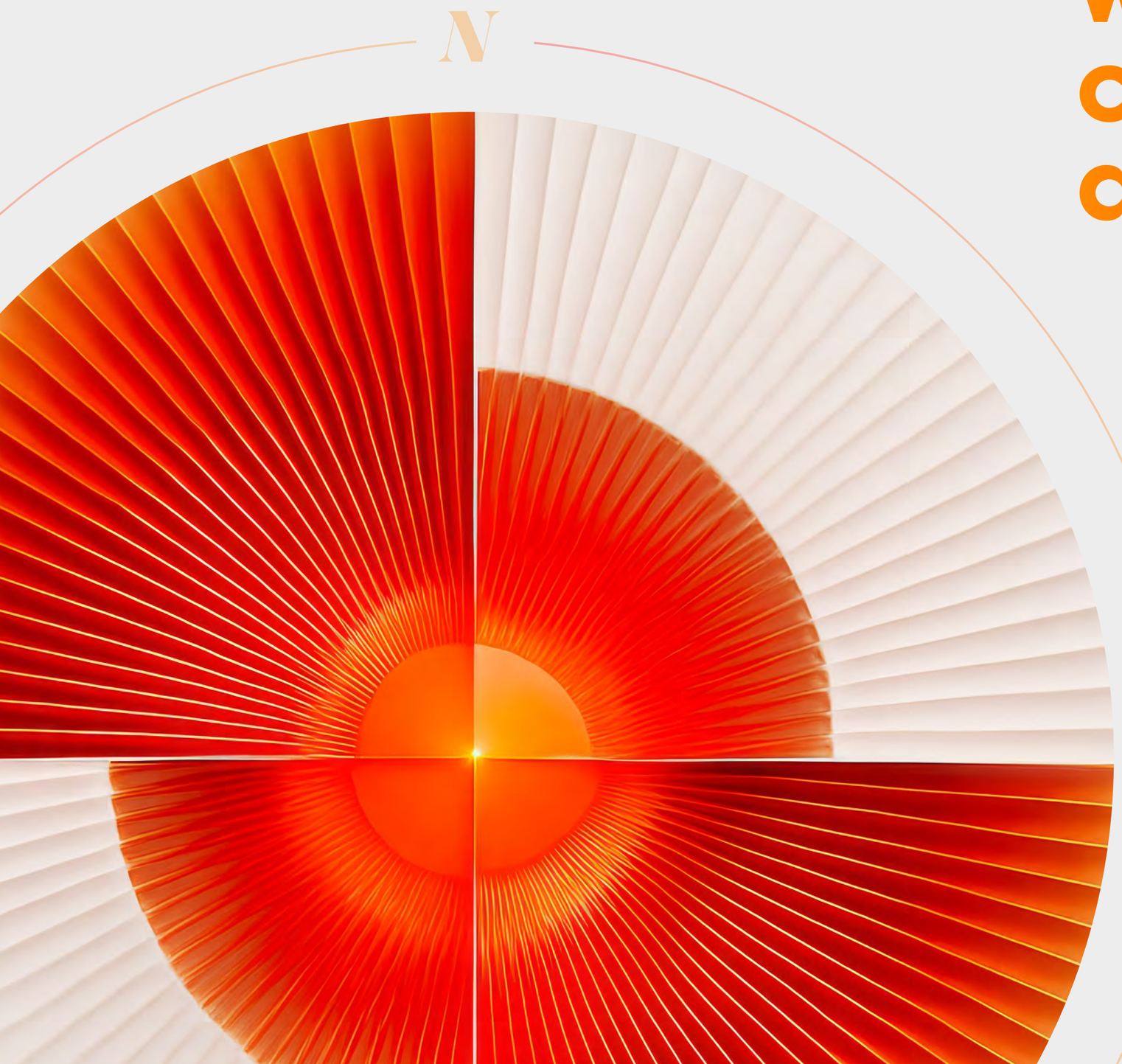


AI is nothing without control and purpose

From data governance to decision and sovereign AI governance

CIO Compass Series

Executive framing
— *Why this matters now*

AI governance is reaching a tipping point. Many organisations have deployed governance actions initially to satisfy regulatory and compliance requirements. But GenAI and agentic systems are pushing data far beyond reporting pipelines into automated decision loops — where business value, risk, and cost are created (or destroyed) in real time.

- Many data governance programs were designed for regulated data and auditability — not to maximise business outcomes.
- The regulatory approach has clear limits: business data that drives revenue, customer experience, and operations needs the same level of discipline — but with measurable value, not paperwork.

AI only creates value when it operates within clear boundaries: *purpose, responsibility, sovereignty.*

- Governance ROI is increasingly questioned: heavy documentation and controls on narrow scopes are hard to justify without visible impact.
- Governance must not slow innovation; it must secure it so industrialisation becomes faster, safer, and repeatable.
- Self-service data and more autonomous users increase risk exposure (leaks, breaches, confidentiality issues) and demand reinforced governance, especially for sensitive domains.
- GenAI exposes governance weaknesses: LLMs and RAG act as a revealing lens, highlighting poor data quality, outdated definitions, inconsistent access rules, and unclear accountability.
- Agentic AI increases the risk profile: modular agents, agent-to-agent communication, dynamic tool use, and distributed AI meshes require a new generation of governance rules.

Governing AI is *governing power.*

Introduction:
The Illusion of Control

Over the past decade, most large organisations have invested heavily in data governance. Catalogues were deployed. Quality rules documented. Access rights formalised. Committees installed.

And yet, as AI enters the core of operations, a disturbing reality is emerging: **most organisations govern data, but not decisions.**

Traditional data governance was initially designed to satisfy regulators, not to scale decision-making. It focused on assets, not outcomes. On documentation, not responsibility. On compliance, not performance.

AI fundamentally breaks this model.

AI systems no longer support decisions at the margin. They influence, recommend, prioritise — and increasingly **execute** decisions at scale. When decisions scale, responsibility must scale with them. And when responsibility is unclear, risk grows exponentially.

This is why governance can no longer be treated as an administrative layer or a compliance afterthought. It has become **a performance discipline.**

AI acts as a brutal revealer. Large Language Models and Retrieval-Augmented Generation expose what legacy governance tried to mask: poor data quality, outdated definitions, inconsistent access rules, blurred ownership. These weaknesses are no longer theoretical — they directly degrade outcomes, trust and economics.

With the rise of agentic AI, the challenge deepens further. Autonomous systems move from analytics to action, from insight to execution. Governance must therefore become **explicit, operational and enforceable** — not declared after the fact.

Sovereignty, in this context, is no longer a cloud debate. It is **a decision-control issue.**

AI only creates durable value when it operates within clear boundaries: **purpose, responsibility and sovereignty.**

Client case

Scandinavian energy company

Data Governance to Drive Efficiency and AI Readiness

Context
Data fragmentation, inconsistent information, and low trust—combined with a complex post-M&A systems landscape—were limiting operational efficiency and slowing digital and AI initiatives.

Actions
A modern cloud-based data platform was deployed, supported by structured governance frameworks and embedded stewardship roles. Governance was aligned with enterprise architecture and Microsoft Purview to ensure security and compliance, while cultural adoption was reinforced through training and change management.

Results
Time spent on data validation decreased, data quality and reliability improved through clear ownership and master data management, and confidence in digital and AI tools increased. The organization gained a scalable foundation for advanced analytics and AI-driven decision-making.

Takeaway
AI value depends on a strong data foundation. Technology is critical—but governance, ownership, and cultural adoption are what ensure sustainable impact.

The end of naive AI
— Why control and purpose are strategic

Agentic AI raises the bar further. Ownership must be explicit: who defines business rules, who builds and validates the agent, who authorises sensitive actions, and who remains accountable when autonomy escalates.

This is where organisations either enter a vicious cycle — poor data quality, irrelevant data products, long time-to-value, low adoption — or a virtuous one where mastered data assets unlock high-value experiences, faster decisions, and compounding impact..

- → Relevant data and AI products that match real operational needs.
- → Higher user value and trust, improving adoption and reducing shadow usage.
- → Time-to-Value acceleration through reusable, certified assets and clear ownership.

AI does not understand intent. It amplifies patterns.

Data carries no purpose. Organisations do.

This misunderstanding lies at the heart of many failed AI initiatives: the belief that intelligence will emerge automatically from data and models. In reality, AI accelerates what already exists — fragmentation, bias, weak ownership, unclear accountability and hidden cost structures.

More AI without control does not create intelligence. It creates **scaled risk.**

Speed without purpose does not create value. It creates **noise, volatility and cost drift.**

Agentic AI makes this explicit. When systems can reason, plan and act autonomously, governance must answer uncomfortable but unavoidable questions:

When Speed Creates Noise

Decision Volatility

Uncontrolled proliferation of AI models and self-service usage drives **inconsistent, unstable, or conflicting decisions** across systems and teams.

Decision volatility directly translates into operational friction and cost drift.(1)

- → **Who defines the rules an agent follows?**
- → **Who authorises its actions and scopes its autonomy?**
- → **Who supervises its behaviour in real time?**
- → **Who is accountable when it fails, drifts or causes harm?**

Organisations that do not answer these questions explicitly are not innovating faster — they are **delegating responsibility without ownership.**

AI accelerates what you already are. Without control, it scales chaos.

(1) In the AI era, business governance means safeguarding trust | World Economic Forum Artificial Intelligence Requires an Extended Governance Framework

From data governance *to decision governance*

Data governance and data cleansing are the essential first steps of any AI initiative. Ownership and data quality come first – because every automated decision is only as reliable as the certified data products feeding it. Pragmatism is key: start from the business outcome, derive the minimum data scope required to deliver measurable value, then govern that scope deeply – rather than attempting to govern all data equally.

Traditional data governance protects assets. AI governance must govern **decisions and their consequences.**

Every AI system influences a decision. Every decision has:

- a business owner,
- a level of risk,
- an economic, operational and reputational impact.

This requires a fundamental shift:

Govern the decision, not the dataset.

Data quality, lineage and access control are not optional prerequisites – they are the foundation of any serious AI initiative. But they are insufficient if they are not explicitly connected to decision ownership and accountability.

Without a named decision owner, AI governance remains theoretical.

Organisations must now classify decisions explicitly:

- **Which decisions can be automated end-to-end?**
- **Which must remain supervised by humans?**
- **Which should never be delegated to machines?**

If an organisation cannot answer these questions clearly, it is not governing AI. It is merely observing it.

Where Control Really Starts

Decision Governance Coverage

Less than 20% of AI-influenced or AI-executed decisions have a **clearly assigned business owner,** explicit decision rules, and formal accountability.

Data governance is widespread. Decision governance remains largely unaddressed.[2]

The three pillars of trusted data *– Foundations of AI*

Trusted data is not an abstract quality label. It is the foundation that makes decisions auditable, models governable, and AI industrialisable.

- **Quality** – The quality of decisions never exceeds the quality of inputs.
- **Lineage** – If you can't trace the data, you can't justify the decision.
- **Control** – Knowing who accesses data is knowing who controls decisions.

AI performance never exceeds the quality of its inputs.
But quality alone is not enough.

(2) Artificial Intelligence Requires an Extended Governance Framework
AI Governance Frameworks For Responsible AI | Gartner Peer Community

Three pillars define trusted data in the age of AI:

Quality

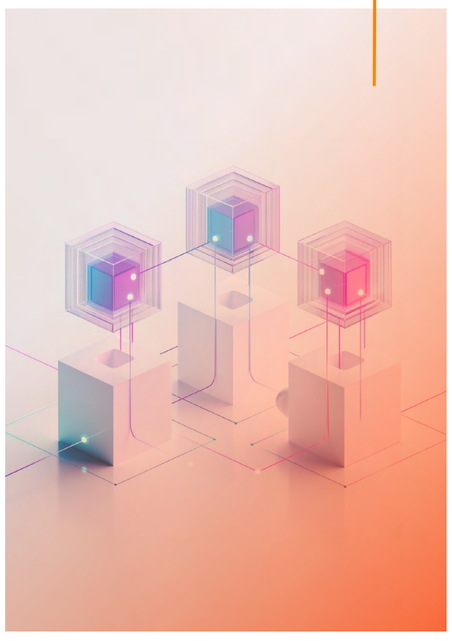
AI does not fix bad data. It amplifies it. Poor inputs produce confident but wrong outputs, at scale.

Lineage

Traceability is the foundation of accountability. If data cannot be traced, decisions cannot be justified — legally, ethically or operationally.

Control

Access defines power. Uncontrolled access creates legal, ethical and strategic risk.



Knowing who can access data is knowing who can influence decisions.

Trusted data is therefore not a technical attribute. It is a **governance commitment.**

Client case

AI and Data Quality: From Detection to Remediation

A large financial services organisation was manually reviewing more than 200,000 contracts within a limited time frame (six hours), relying on multiple data sources and fragmented processes. This created significant exposure: undetected errors, anomalies identified too late, potential regulatory penalties, and financial losses.

Approach Implemented

The organisation launched a Proof of Concept on historical data, combining:

- AI algorithms (Isolation Forest and supervised models) to detect anomalies and cluster suspicious contracts.
- Business intelligence visualization tools to explore, interpret, and validate detected patterns.
- A progressive industrialization approach, including hot and cold processing, CI/CD integration, and gradual scope expansion.

Results Achieved

- 14,000 erroneous contracts identified (previously undetected).
- €2 million in misclassified outstanding amounts uncovered.
- Potential exposure estimated at up to €20 million in case of non-compliance.
- Processing cycle reduced by four hours (approximately –40%).
- Around 3% annual time savings.

Conclusion: Demonstrated ROI and validated solution, successfully transitioning from manual controls to automated and industrialised anomaly detection.

Model governance *— The missing layer*

AI models enrich the enterprise digital estate: they are new high-value assets that must be treated and governed as products — with lifecycle, owners, and explicit replacement paths.

Model governance is not AI project prioritisation. It is decision rights: what models and agents are allowed, under which policies, with which ethics, and with what level of auditability.

Economics are deeply shaped by model choice. Defaulting to large general-purpose models can inflate the bill; disciplined organisations benchmark and use the smallest effective model (including specialised small language models) where possible. At scale, governance must operate in an industrial mode: full model registry and versioning, observability and alerting, security and compliance controls, robustness testing, explainability, guardrails, and agentic orchestration policies.

Models are not experiments. They are decision engines. They drift. They evolve. They embed assumptions. They create dependency.

Yet many organisations still treat models as temporary projects rather than strategic assets.

Model governance is not about prioritising AI initiatives. It is about **decision rights, lifecycle management and economics.**

Choosing a model determines:

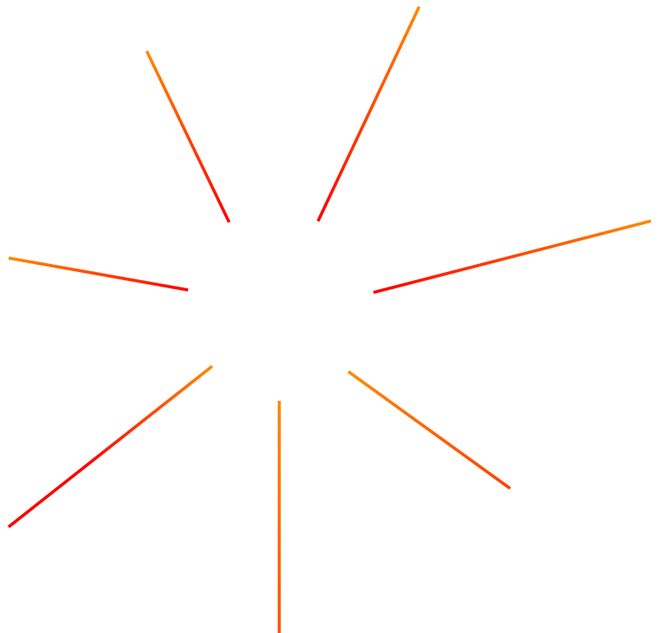
- cost structures and volatility,
- sovereignty exposure,
- explainability limits,
- replacement difficulty.

Defaulting to large, general-purpose models where smaller, specialised ones would suffice inflates costs and carbon footprint without improving outcomes.

A model without an owner is unmanaged risk.

Effective AI governance therefore requires industrial discipline: registries, versioning, observability, security controls, explainability mechanisms, cost attribution and explicit exit strategies.

Vendor lock-in has moved from infrastructure to cognition — and cognition is far harder to reverse.



Governing agentic AI — *From outputs to behaviours*

Agentic AI forces a shift from compliance governance to performance governance. We no onger govern static assets (datasets, models) — we govern dynamic behaviours: action chains, decision sequences, and degrees of autonomy.

Governance becomes operational housekeeping: tracking who uses which agent, what tools it can access, what it is allowed to do, and how costs are attributed and contained.

- Explicitly define allowed and prohibited zones for GenAI, autonomous agents, and automated actions on the information system.
- Govern system prompts, RAG corpora and tool access (permissions are part of governance).
- Implement real-time guardrails, monitoring and kill switches to maintain control and ensure safe operation.
- Prepare for AI mesh dynamics: modular agents, agent-to-agent communication, and dynamic sourcing require consistent policies across the chain.

Agentic AI changes the nature of risk.

Traditional governance focuses on inputs and outputs. Agentic AI requires governing **behaviour,** not just results.

The risk is no longer a wrong answer. It is a **legitimate action executed at scale,** potentially across systems and processes.

Governing agentic systems means:

- defining allowed and forbidden action zones,
- controlling tools, permissions and execution rights,
- governing system prompts and knowledge sources,
- implementing real-time guardrails, monitoring and kill switches.

If an organisation cannot stop an AI agent in real time, it does not govern it. It merely observes it.

When Scale Becomes Fragility

AI Risk Amplification

A human error is contained.
An uncontrolled AI error **propagates instantly and at scale.**

Automated decision failures can affect **10 to 100 times more operations, customers, or revenues** than traditional IT incidents.[3]

AI governance *meets sovereignty*

Sovereignty is practical. It is the ability to demonstrate compliance and control at any moment – and to keep options open when vendors, geopolitics, or regulations shift.
Implications for CIOs:

- Master cross-border data flows and document where sensitive data is processed.
- Ensure cloud reversibility and model portability (avoid single-model dependency).
- Maintain end-to-end traceability of AI usage and decisions to prove control on demand.

Vendor lock-in has moved *from infrastructure to cognition.”*

Layer	*Sovereignty question*
Data	*Where is it stored and who can access it?*
Models	*Who trains, updates and controls them?*
Platforms	*Who operates the infrastructure?*
APIs	*Who controls the interfaces and pricing?*
Decisions	*Who is legally accountable?*

Sovereignty is not a slogan.
It is the practical ability to retain control over **data, models, platforms and decisions.**

The new sovereignty stack is explicit:

- **Data:** where it resides and who accesses it
- **Models:** who trains, updates and replaces them
- **Platforms:** who operates the infrastructure
- **APIs:** who controls interfaces, pricing and dependency
- **Decisions:** who is legally and operationally accountable

Loss of sovereignty rarely happens at once.
It happens through irreversible architectural choices: external fine-tuning, opaque APIs, single-model dependencies.

Once cognition is outsourced, sovereignty becomes theoretical.

Control, Not Infrastructure

Decision Sovereignty

AI sovereignty is not defined by where models run, but by **who controls, explains, and arbitrates automated decisions.**

Most organisations lack explicit ownership and control over their most critical AI-driven decisions.[4]

(3) WEF_Artificial_Intelligence_and_Cybersecurity_Balancing_Risks_and_Rewards_2025.pdf

(4) Making sense of AI frameworks | PwC Switzerland
2025-ICC-Policy-Paper-AI-governance-and-standards.pdf

AI Act — *A reality check for AI governance*

The AI Act will not automatically accelerate innovation. It will expose organisations unprepared for governance — and it can become a catalyst to strengthen data and AI product governance when treated as a structuring framework, not a checklist.

Three hard realities must be acknowledged:

- Ambiguity of requirements — key notions (high-risk systems, transparency) will be learned in practice, not on paper.
- Shortage of expertise — AI governance requires rare hybrid skills (legal, data, AI, risk) that are scarce.
- Aggressive timelines — two years is extremely tight for complex, legacy-heavy environments; the calendar assumes a maturity most organisations do not yet have.

The impact will be disproportionate for SMEs: limited financial buffers and scarce expertise mean compliance can absorb a large share of R&D capacity. As with GDPR, effort and cost are widely underestimated — for many SMEs, compliance becomes a survival problem.

Sanctions are severe and comparable to GDPR, but the AI Act is more complex and less mature. The primary risk is no longer malicious non-compliance — it is accidental non-compliance.

End-to-end traceability becomes mandatory:

Data → Transformations → Features → Model → Decision → Action

These requirements can only be met if data metadata natively feeds AI governance and usage policies remain consistent across the entire chain.

Concrete implications: organisations need the technical ability to:

- Reconstruct AI reasoning, explain automated decisions, and suspend non-compliant models.
- Centralise Data & AI logs for audit, oversight, and incident response.
- Enable on-demand audit capabilities (regulator requests, internal controls, major incidents).

Use the AI Act as a design standard:

- Classify AI use cases by risk level and align controls with that risk.
- By default, fully document every high-risk AI system.
- Embed compliance by design into pipelines and platforms — waiting for clarity is the most expensive strategy.

Regulation will not slow AI adoption. It will expose ungoverned organisations.

The real challenge is not interpretation, but **traceability:** from data to features, from models to decisions, from actions to outcomes.

Compliance by design beats compliance by panic.
The AI Act will not reward those who wait for clarity.
It will favour those who embed governance into architectures, pipelines and operating models.

Anything else will collapse under scale.

Client case

Trustworthy AI: supporting organisations in achieving European compliance

As a member of the AI PACT, Sopra Steria implemented this regulation ahead of schedule for all our proprietary activities. To do so, we developed AI risk assessment and mapping tools, methodologies for structuring compliance plans, and training courses dedicated to the AI Act. Drawing on our own experience and fueled by our active participation in industry groups responsible for defining application standards, we are already supporting several of our clients in their AI Act program with a comprehensive and proven approach to managing compliance with new data/tech regulations (GDPR, DORA, NIS2, etc.): raising awareness and training teams, mapping AI uses and their risks, clarifying roles (developer, integrator, user), auditing and reducing risks, integrating compliance "by design" into business and IT processes. Beyond compliance, Sopra Steria Next helps its clients build a true culture of trust and responsible innovation — as shown by our references with Amazon Logistics (trainings on current AI issues and challenges, the fundamentals and key principles of AI, preparing use cases according to the business needs, raising awareness of AI regulation: the AI Act) or BNP Paribas (managing security projects at the GDPR program management level and minimising data and consent policy).

The CDAIO
— *The new leadership role*

The CDAIO is no longer just a technical expert. It is a BizTech leader who anchors ethics, compliance, sustainability and architecture into day-to-day execution — speaking the language of operations, finance, legal and IT.

What the CIO must explicitly refuse:

- AI models trained on non-certified data.
- AI POCs running outside governance frameworks.
- Purely declarative governance (documentation without executable controls).
- AI tools disconnected from the data catalog and metadata ecosystem.

Recommended steering indicators:

- % of AI models trained on certified datasets.
- % of automated decisions that are fully auditable end-to-end.
- Number of AI incidents caused by data issues (quality, access, lineage).
- Time required to document a model during an external audit.

A deep redistribution of roles is underway: business teams become accountable for data and AI products, CDAIOs embed governance into the target architecture, and AI teams become responsible for the behaviours of the systems they design — including human-in-the-loop when needed.

From Insight to Accountability

Decision Traceability & Replay

Fewer than 25% of AI-driven decisions in production can be **fully traced, audited, and replayed end-to-end,** at a level comparable to critical IT transactions.

Without decision traceability, operational control and regulatory readiness are fragile.[5]

(5) Making sense of AI frameworks | PwC Switzerland
2025-ICC-Policy-Paper-AI-governance-and-standards.pdf

Empowering the organisation requires decentralised autonomy with strong guardrails: business teams own data products; data champions and stewards sit close to operations; and stewardship can be activated or deactivated depending on the domain and outcome.

Operating through concrete tools is essential: offensive governance via the data catalog (track active monthly users), lineage coverage KPIs, and end-to-end visibility across the full data lifecycle.
The Chief Data & AI Officer is not a renamed CDO, nor a super data scientist.

It is a **BizTech arbitration role.**

The CDAIO resolves structural tensions:

- **between speed and control,**
- **between innovation and sovereignty,**
- **between compliance and performance.**

This role is not consensual by nature. It exists to make responsibility explicit — and sometimes to say no.

Data and AI governance is no longer an IT responsibility.
It is a **business leadership responsibility.**

Shadow AI, *shadow models, shadow data*

AI spreads faster than governance. Shadow usage appears through unmanaged tools, rogue prompts, unofficial RAG corpora, and quick model fine-tuning. The result is predictable: broken traceability, uncontrolled cost, and sovereignty loss before leadership even notices.

The greatest AI risk is not what IT builds. It is what the organisation uses unknowingly.

Shadow AI destroys traceability, sovereignty and cost control before leadership even notices.

Ungoverned AI first destroys budgets. Then trust.

What mature organisations *do differently*

Mature organisations reset governance around outcomes. They govern what matters for measurable business performance — and apply minimum viable governance to non-critical data, using exception-based controls.

They industrialise governance as an architecture discipline:

- Embed governance into target Data, AI and GenAI architectures (RAG patterns, agent orchestration, pipelines).
- Reject any AI system that lacks traceability, observability and access/action control — a system that cannot be governed is not eligible for industrialisation.
- Shift from declarative to executable governance: translate rules into automated controls, CI/CD tests and platform policies. At scale, a rule not implemented in the pipelines simply does not exist.
- Use AI to accelerate governance: automate classification, cataloging, lineage and quality checks; detect anomalies; reduce manual effort.
- Integrate Data as a Product (DaaP): semantic layers and data contracts guarantee structure, quality and availability.

Pragmatism is the discipline:

balance agility **VS** *control*
speed **VS** *compliance*
data openness **VS** *sovereignty*
performance **VS** *ethics*

Mature AI organisations *say no more often than yes.”*

- limit AI usage by design,
- classify decisions by criticality,
- assign business ownership to models,
- measure impact, not just accuracy,
- design for reversibility and sovereignty.

They say no more often than yes.

Separating Industrial AI from Experimentation

AI Value Realisation Rate

Only **20–30%** of AI use cases deliver a **measurable and sustained business ROI** 12 to 18 months after production deployment.

Speed without governance increases activity — not value.[6]

Anti-patterns *to avoid*

Common traps CIOs must actively avoid:

Seeing governance as a cost, not a value lever.

The one-shot cleaning fallacy: believing a single big data cleanup is enough.

Heavy governance perceived as constraint (months of documentation) with no visible business impact

Perfection obsession: waiting for 100% quality everywhere instead of targeting the critical data first.

Dissociating data governance and AI governance — they are one chain.

Implementing Governance after deployment

Leaving data responsibility to IT alone instead of business ownership of data products.

(6) The State of AI: Global Survey 2025 | McKinsey
AI's 2025 Reality: Widespread Adoption, Narrow Impact, and the High Performers' Edge
BCG Says Only 5% of Companies Are Seeing Value From AI. Here's Why. - Business Insider

Recommendations — *Call to action*

Governance is not here to police data; it is here to unlock its potential. In the agentic era, ungoverned data becomes unusable data — because you cannot trust, audit or industrialise automated decisions.

- → **Adopt a value-first approach:** govern only what directly supports priority business outcomes to secure ROI and avoid team burnout.
- → **Fuse data and AI governance:** AI governance is the extension of data governance. Avoid silos — agent behaviour reflects your data estate.
- → **Automate documentation with AI:** turn yesterday's manual burden into a dynamic flow of metadata.
- → **Make business teams accountable for their data products:** bad data captured today becomes a failed automated decision tomorrow.
- → **Name Data Product Owners:** assign business owners accountable for quality and fitness-for-use.
- → **Shift from control governance to access governance:** make reliable data instantly available so innovation can happen safely.
- → **Demonstrate governance value with an Agentic Safe pilot:** deploy an agent on a restricted but perfectly governed scope to prove scale and speed.
- → **Invest in lineage:** ensure every AI decision can be traced back to its original data sources for auditability.

WE PROPOSE TO RELY ON OUR 9 DIMENSIONS FRAMEWORK TO ASSESS CURRENT-STATE AND DESIGN FUTURE-STATE ALLIANZ TECHNOLOGY DATA STRATEGY

01
Vision & economics

02
Operating model

03
Skills & culture

04
Use cases

05
Data & AI portfolio

06
Data & AI governance

07
Risk, compliance, ethics & sustainability

08
Technology & capabilities

09
Sourcing & partenership

Conclusion
— *Governing AI is governing power*

Final reminders for CIOs:

- AI is nothing without control and purpose.
- Without sovereignty, AI creates dependency.
- Only governed AI creates durable value.

AI is not a technology problem.
It is a leadership, responsibility and sovereignty problem.

Manual, declarative or retrospective governance does not scale.
If a system cannot be governed, it cannot be industrialised.
AI is nothing without control and purpose.
Without sovereignty, it creates dependency.
Only governed AI creates durable value.

The critical question for every CIO is no longer:
"Can we deploy AI?"

It is:

"Which decisions in our organisation are already made by AI — without anyone formally owning them? "

Contacts

Valérie THIBLET
Partner Head of Data & AI
→ valerie.thiblet@soprasterianext.com

Alexandre RIETHMULLER
Senior consultant IT Strategy & Big Data
→ alexandre.riethmuller@soprasterianext.com

Contributors of our European Network

Olivier BROUSSEAU
Architecture & Tech
→ olivier.brousseau@soprasterianext.com

Isabelle PONS
Data & AI
→ isabelle.pons@soprasterianext.com

Valérie THIBLET
Data & AI
→ valerie.thiblet@soprasterianext.com

Axelle ROESCH
CIO Advisory
→ axelle.roesch@soprasterianext.com

Thomas OTTO
CIO Advisory
→ thomas.otto@soprasteria.com

Philipp MAIER
CIO Advisory
→ philipp.maier@soprasteria.com

Simon KAYE
Architecture & Tech
→ simon.kaye@soprasteria.com

Ray BAKER
Architecture & Tech
→ ray.baker@soprasteria.com

Andy WHITEHURST
Architecture & Tech
→ andy.whitehurst@soprasteria.com

Eirik HASLESTAD
CIO Advisory
→ eirik.haslestad@soprasteria.com

Jahn-Fredrik SJOVIK
CIO Advisory
→ jahn-fredrik.sjovik@soprasteria.com

Tor NESET
Architecture & Tech
→ tor.neset@soprasteria.com

Marius SANDBU
Data & AI
→ marius.sandbu@soprasteria.com

Robert HEXSPOOR
Architecture & Tech
→ robert.hexspoor@soprasteria.com

Hugo HERMSEN
CIO Advisory
→ hugo.hermsen@soprasteria.com

Juan Antonio MARTINEZ SANCHEZ
Architecture & Tech
→ juanantonio.martinezsanchez@soprasterianext.com

Mauro PALMARINI
CIO Advisory
→ mauro.palmarini@soprasterianext.com

Conception: Spintank, photos credits: GettyImages ©