Data Integrity in B2B: From Noise to Trust

How Enterprise Truth Determines Performance, Governance and Competitive Advantage

Mark Conway, Oak Consult

May 2026

Contents

Foreword

By Mark Conway, Oak Consult

Most organisations do not have a shortage of data. They have a shortage of truth.

That may sound blunt, but it is the problem I keep seeing. Boards are shown dashboards, leadership teams are given reports, and functions arrive at review meetings with numbers they can defend. Marketing has its version, Sales has its version, Delivery has its version, and Finance often has another. Everyone can explain their position, which is precisely why the problem can last so long.

The customer, meanwhile, is living with the consequences.

They are having to repeat information to one department that they have already provided to another, waiting for updates that should have been proactive, and discovering that what was sold, implemented and serviced can feel like three different promises. Internally, the metrics may still look green. Externally, the relationship can feel anything but healthy.

That is why this paper matters.

Data integrity is too often treated as a technical issue — something for IT, data teams, or transformation programmes. That is a mistake. If the information reaching leadership is fragmented, inconsistent, late, duplicated, or quietly massaged into something more comfortable, this is not just a data problem. It is a control problem, and control is a board-level issue.

I've sat through enough leadership meetings and post-mortems to know exactly how this happens. It is almost never malicious. Most of the time, good people are doing their best with disconnected systems, inherited processes, unclear ownership, and reporting habits that have become normal. The problem is that "normal" can become expensive very quickly.

A forecast that needs constant explaining, a customer view that no one quite trusts, a pipeline that looks strong but does not convert, or a service report that says performance is fine while customers are quietly losing confidence — none of these may look catastrophic on its own. Taken together, they tell you something important: the organisation is not operating from a reliable version of reality.

At Oak Consult, we talk a lot about putting on the Customer Spectacles. That does not mean being soft, sentimental, or blindly customer led. It means having the discipline to see what the customer is actually experiencing, not what the organisation would prefer to believe.

The same principle applies to data. If your dashboards tell one story and your customers are living another, the dashboard is not the truth; it is only part of the evidence.

The uncomfortable question for any CEO is simple: can I trust the version of reality this business is using to make decisions?

If the answer is “not entirely”, then the next question is not about systems. It is about ownership. Who owns the truth? Who reconciles it? Who has the authority to challenge the numbers when they do not match the customer, the operation, or the commercial outcome?

This paper argues that data integrity must move out of the technical background and into the leadership foreground. Not because data is fashionable, and not because AI has made everyone nervous, but because decisions are only as strong as the reality they are based on.

AI makes this even more urgent. If your underlying truth is fragmented, AI will not magically fix it. It will accelerate it. It will scale the assumptions, repeat the errors, and expose the weaknesses faster than your governance can explain them away.

The real risk is not that the data is imperfect — every organisation has that. It’s that leadership pretends the imperfect data is good enough while staying blind to where the weaknesses are, what they’re costing, and who should be fixing them.

This paper is not written for data specialists. It is written for leaders who need to make better decisions, faster, with fewer excuses and less hidden friction. It is written for CEOs, CFOs, COOs, commercial leaders, transformation leaders, and anyone else who has ever sat in a meeting thinking: “These numbers look right, but something still feels wrong.”

If that thought has crossed your mind, it is worth listening to, because customers usually feel the gap before the board sees it. Frontline teams usually work around it before leadership names it. Performance usually drifts before governance catches up.

The purpose of this paper is to make that drift visible. Not to create fear, not to sell a system, and not to add another layer of management theatre, but to help leaders ask a harder and better question:

Are we managing the business from truth, or from noise?

If it is truth, strengthen it. If it is noise, govern it.

Because in the end, growth built on unreliable reality does not scale. It just gets better at hiding the problem.

Executive Summary

Many organisations cannot fully trust the version of reality they are using to run the business. That is not because they lack data. In most cases they have more than enough. The issue is how that data is combined, interpreted, and presented. What reaches leadership is often a constructed view of performance — coherent enough to support decisions, but not always robust enough to withstand real pressure.

The impact rarely appears as a single dramatic failure. Instead it shows up in slower decisions, inconsistent forecasts, misallocated capital, and customer outcomes that fail to match internal reporting. Over time this creates a persistent gap between what the numbers say and what is actually happening.

Even conservative modelling indicates that organisations operating on fragmented or unreliable data are exposed to a 5–10% performance drag. At scale, that represents tens or hundreds of millions in distorted decisions, delayed action, and missed opportunity. Treat the range as a scenario-based exposure model rather than an audited loss figure. Its purpose is to help leadership test materiality. This is not a data quality issue. It is a control issue.

When the underlying version of reality cannot be trusted, governance becomes interpretive rather than decisive. Leadership conversations shift from “what should we do?” to “which numbers do we actually believe?” The organisation absorbs friction at every level. The risk is increasing. Artificial intelligence does not fix these conditions — it amplifies them. Automated systems act on the data they are given, scaling both the strengths and the weaknesses at speed. At the same time, regulatory expectations around data governance and accountability continue to tighten. The organisations that respond effectively do three things:

1. Establish clear ownership of their version of reality, rather than allowing multiple functional perspectives to coexist unchecked.
2. Implement governance that forces reconciliation, surfacing and resolving contradictions instead of managing them in isolation.
3. Define measurable data integrity as a business condition, making confidence levels visible and actionable.

This does not require a multi-year transformation programme. A structured 90-day control reset can establish ownership, make integrity visible, define the core truth model, and embed a governance cadence that aligns with how the business actually runs. From there, improvement becomes continuous. Organisations that can trust their version of reality make faster decisions, allocate capital more effectively, and respond to change with greater confidence. Over time this creates a measurable performance advantage.

Those that cannot continue to operate with hidden friction — cost and variability that rarely appear explicitly on any report but are felt consistently across the business. This paper is structured as a leadership argument, not a technical guide. It moves from the economic cost of distorted truth, through governance risk and performance implications, to the architecture, implementation approach, and board-level decisions required to move from noise to controlled reality.

I. Truth, Noise and Economic Distortion

I.0 Framing — From Data to Truth

Most organisations believe they have a data problem. They talk about quality, completeness, integration, and reporting. They invest in platforms, build dashboards, and run transformation programmes designed to bring everything together. The language is familiar: “single source of truth,” “data-driven decision-making,” “improved visibility.”

Yet despite all of this, something still does not quite hold.

Decisions take longer than they should. Forecasts need constant revision. Commercial performance drifts in ways that are hard to explain. Leaders find themselves relying on judgement calls, side conversations, and informal validation rather than the systems they have invested in.

The issue is not that data is missing. It is that the version of reality the organisation is operating on cannot be fully trusted. This is the shift that matters.

Organisations do not make decisions on raw data. They make decisions on what they believe to be true.

I.1 The Hidden Enterprise Cost of Distorted Truth

When that belief is even slightly wrong, the impact does not appear as a single failure. It spreads. Pricing decisions are made on incomplete customer views. Forecasts are built on inconsistent assumptions. Capital is allocated based on performance signals that look credible but do not quite reflect what is happening on the ground. Teams spend time reconciling differences between systems rather than acting on insight.

Individually, these effects are manageable. Collectively, they become material.

This is the silent tax of distorted truth — not a line item on a balance sheet, but a continuous leakage of value across the organisation. It shows up as misallocated spend, delayed decisions, operational inefficiency, and missed commercial opportunity. It is felt in slower growth, weaker margins, and an increasing reliance on workarounds.

The scale is often underestimated because it is distributed. But when modelled at enterprise level, even conservative assumptions make it visible.

These figures are not "losses" in the traditional sense. They represent distortion exposure — the cumulative effect of decisions made on an unreliable picture of reality.

Research from MIT Sloan Management Review and Forrester consistently shows that poor data quality rarely fails at a single point. It compounds downstream, affecting pricing, forecasting, operational efficiency, and ultimately revenue performance.

I.2 The 5–10% Enterprise Reality

The question, then, is not whether distortion exists. It is how much. There is a tendency to look for precise figures — a definitive percentage that can be measured, tracked, and reported. In reality, distortion does not behave that way. It does not sit neatly in one system or one metric. It cuts across functions, decisions, and time.

That is why the 5–10% range is best understood as a modelling discipline, not a fixed claim. It represents a conservative estimate of enterprise-level exposure across revenue leakage, margin erosion, working capital volatility, and executive time spent reconciling rather than deciding.

Importantly, it reflects distortion in decision-making, not just errors in data. Independent benchmarks often suggest significantly higher exposure. Documented cases show nine-figure revenue impacts where data integrity failures cascade through systems and decision processes. Against that backdrop, 5–10% is cautious, but even at that level, the implication is clear: this is not marginal inefficiency. It is a structural performance constraint.

I.3 The AI Multiplier Effect

If distortion was previously contained within human decision-making cycles, that is no longer the case.

Artificial intelligence has changed the dynamics. AI systems do not question the data they are given. They learn from it, optimise against it, and act on it at speed. When the underlying data is coherent and reliable, this creates significant advantage. When it is not, the opposite happens. Errors are not just repeated — they are industrialised.

AI does not create distortion. It scales it. Poor inputs lead to flawed models. Flawed models drive automated decisions. Those decisions then generate new data, reinforcing the original problems. What might previously have been a localised issue becomes systemic and increasingly difficult to unwind.

For leadership, this changes the equation. Data integrity is no longer a background concern. It is a prerequisite for any organisation attempting to operate at speed and scale.

I.4 Distortion Categories — Where It Shows Up

To understand how distortion manifests, it helps to look at where it appears in practice.

Revenue distortion:

Opportunities are misclassified, duplicated, or inconsistently defined. The pipeline looks healthy, but conversion does not follow. Pricing decisions are made without a clear view of customer value or behaviour.

Operational distortion:

Processes appear efficient on paper but require constant manual intervention. Teams reconcile differences between systems, adjust outputs, and compensate for gaps that should not exist.

Forecasting distortion:

Plans are built on assumptions that do not hold. Forecasts are revised frequently, not because conditions have changed, but because the underlying data was never fully aligned.

Customer distortion:

The organisation believes it understands its customers, but the view is fragmented. In wholesale and distribution businesses we have worked with, sales promises one level of availability while operations work to another; customers experience the gap as inconsistency and quietly take their business elsewhere.

Decision latency:

Time is spent validating data, challenging assumptions, and resolving discrepancies. Decisions slow down, not because they are complex, but because confidence in the inputs is low.

Across each category, the pattern is the same. The issue is not a lack of data. It is a lack of a coherent, reliable picture the business can trust.

I.5 Vertical Elasticity — How Distortion Varies

The 5–10% exposure range holds at an enterprise level, but how it manifests varies by sector.

In SaaS and subscription models, distortion often appears early in the customer lifecycle. Onboarding may be reported as successful, yet churn emerges within the first months because adoption and value realisation were never fully captured.

In manufacturing and industrial environments, the tension sits between sales commitments and delivery capability. Orders are booked based on one view of capacity and supply, while operations work to a different one, creating downstream inefficiency and margin pressure.

In wholesale and distribution, complexity in pricing, rebates, and multi-channel fulfilment creates subtle but persistent erosion. Margins appear stable in aggregate, but leakage occurs across transactions and customer segments.

These are not different problems. They are different expressions of the same underlying condition: operating on fragmented truth.

I.6 From Concept to Control — Measuring Integrity

If distortion is accepted as a structural issue, it must be made measurable. This is where data integrity moves from concept to control. At its simplest, integrity can be broken down into five dimensions:

1. Accuracy — is the data correct?
2. Completeness — is anything missing?
3. Consistency — does it align across systems?
4. Timeliness — is it up to date?
5. Uniqueness — is it duplicated or conflicting?

These dimensions are well understood. What is often missing is a way to bring them together into a usable, decision-ready view. This is the role of Oak Consult's Data Integrity Radar. Rather than assessing data in isolation, the Radar evaluates integrity across key domains and translates technical quality into a business-relevant signal. Combined into a single Data Confidence Score, it gives leadership a clear, at-a-glance view of how reliable the organisation's operating reality actually is.

This is where the conversation changes. From: "Is the data good enough?" To: "Can we trust this to make decisions?"

Section I — Closing Position

By this point, the pattern should be clear.

Organisations do not operate on raw data. They operate on constructed versions of reality.

When that construction is coherent and reliable, performance follows. When it is fragmented or distorted, the impact spreads across revenue, operations, forecasting, and customer experience. It is rarely visible as a single failure, but it is consistently felt as underperformance.

The challenge is not recognising that distortion exists. It is accepting that it is structural.

And addressing it requires more than better data. It requires control over how truth is defined, measured, and trusted.

Which brings the issue out of the data domain entirely — and into governance.

II. When Distortion Becomes Governance Risk

II.1 The Trust Threshold

There is a point at which data issues stop being something teams can work around and start becoming a genuine governance concern.

Before that point, inconsistency is inconvenient but manageable. Teams reconcile differences between systems, adjust numbers where needed, and carry enough context in their heads to keep things moving. Decisions may take longer and confidence may not be absolute, but the organisation still functions.

Beyond that point, the dynamic changes. Forecasts begin to require explanation rather than acceptance. Reports come with caveats. Leadership conversations shift away from deciding what to do next and towards questioning whether the underlying numbers can be relied upon at all.

At that stage, the issue is no longer technical. It is structural. The organisation is no longer operating on a version of reality it can trust.

The UK Corporate Governance Code is explicit on the responsibility of boards to maintain effective systems of internal control and risk management. Those systems depend on the integrity of the data that underpins reporting, forecasting, and performance measurement. When that integrity cannot be demonstrated, the control environment is weakened, even if the formal structures remain in place.

This is the trust threshold — the point at which unreliable or fragmented truth stops being an operational irritation and becomes a governance problem.

II.2 Truth Fragmentation as Governance Failure

The earlier pieces in this series explored how customer truth becomes fragmented across functions. Marketing, Sales, and Delivery each produce a version of reality that is internally consistent and credible within its own context.

The problem is not that these views exist. The problem is that they are never fully reconciled.

In the absence of clear ownership, the organisation ends up holding several parallel versions of the truth. Each one is valid from a functional perspective, but none is complete. Leadership receives a set of perspectives rather than a single, authoritative view.

Over time, this becomes normal. Variances are explained instead of resolved. Differences between systems are acknowledged but left in place. Reports are accepted with the understanding that they are directionally useful, even if not entirely aligned.

What looks like pragmatism is, in reality, a shift in how governance operates. Instead of asking "Is this an accurate representation of what is happening?", the organisation starts to ask "Which version of this are we comfortable using?"

The disconnect is often stark. Marketing reports record-low cost-per-lead and surging Marketing Qualified Leads; Sales data shows 80% of those leads fall outside the ideal customer profile with near-zero conversion. Finance sees a Tier-1 client paying on time; Support has logged 50+ critical bugs in 30 days. Logistics reports "optimal" stock levels; Sales has just signed three major deals not yet visible in the ERP.

From the customer's perspective, these silos do not feel like "technical debt." They feel like incompetence.

- After a three-month sales cycle and multiple discovery calls, the implementation team opens the kick-off meeting with: "So, what are you actually looking to achieve?" (the "amnesia" onboarding).
- A customer battling a Severity-1 outage receives an automated upsell email the same week (the "insulting" upsell).
- They update their billing address with their account manager, only to receive a late-payment notice sent to the old address three months later (the "paperwork" paradox).

This is the customer-facing "Silo Tax": extra time, frustration, and eroded trust because your internal data cannot keep up with the relationship.

When customer truth is not governed, data integrity failures do not appear as isolated issues. They become a structural feature of how the organisation operates.

II.3 Performative Governance

Most organisations, even at this stage, would still describe themselves as well governed. There are reporting packs, dashboards, review meetings, and escalation routes. Metrics are defined, tracked, and discussed. From the outside, the structure appears robust.

The difficulty lies in what those structures are operating on.

If the underlying picture is inconsistent or fragmented, governance processes continue to run — but without a stable foundation. Reports are produced on time, yet require explanation. Metrics are compared, but not always on a like-for-like basis. Meetings take place, but often focus on understanding discrepancies rather than resolving them.

The result is a form of governance that looks active but struggles to exert real control. Performance appears stable in reports, while issues build quietly in the background. Targets are met, but not always in ways that translate into sustainable outcomes. Customer experience can deteriorate without triggering an immediate response, because the signals that would normally surface the problem are diluted or misaligned.

The problem is not the absence of governance structures. It is that those structures are operating on a version of reality that has not been fully reconciled.

II.4 AI × Governance Risk

The introduction of AI into this environment changes the nature of the risk.

Automated systems rely on the data they are given. They identify patterns, optimise against defined objectives, and generate outputs that feed directly into decisions and actions. When the underlying data is coherent, this creates consistency and speed. When it is not, those same characteristics work in the opposite direction.

Decisions are made more quickly, but the underlying assumptions may be flawed. Errors are repeated across systems rather than contained. Patterns of inconsistency are reinforced because the models are learning from the same distorted inputs.

What would previously have been identified and corrected through human judgement can become embedded and much harder to unwind.

AI does more than amplify existing issues — it exposes them faster and at greater scale. For leadership, this creates a different kind of exposure. The organisation may appear more advanced and automated while becoming more dependent on a version of reality that has not been fully validated.

Regulatory expectations are evolving in parallel. Organisations are increasingly expected to demonstrate that their data governance and automated decision-making processes are effective. Without a reliable foundation, that demonstration becomes difficult — if not untenable.

Section II — Closing Position

The progression from data inconsistency to governance risk is rarely immediate, but it is consistent.

What begins as fragmented truth moves through the organisation, shaping reporting, influencing forecasts, and informing decisions. Initially the impact is absorbed through experience and workarounds. Over time, however, confidence erodes gradually. Numbers require more explanation. Decisions require more validation. The gap between what is reported and what is actually experienced — both internally and by the customer — becomes harder to ignore.

At that point, governance is no longer anchored in a stable understanding of reality. It is operating on assumptions that have not been fully reconciled.

This is where data integrity moves out of the domain of systems and into the domain of leadership.

III. Trust as a Performance Condition

III.1 From Insight to Control

Most organisations believe that better data leads to better insight, and that better insight leads to better decisions. That logic holds — up to a point. The missing step is control.

Insight on its own does not change outcomes. It informs them. It highlights patterns, surfaces opportunities, and identifies risks. But unless that insight is grounded in a picture of reality the organisation can actually trust, it rarely translates into consistent performance.

This gap is well documented. Research from MIT Sloan Management Review shows that organisations with high confidence in their data execute decisions more quickly and consistently. Those with lower confidence fall into cycles of validation, rework, and delay.

An organisation can be rich in insight and still struggle to execute. It can see the issues, understand the dynamics, and even agree on the right course of action — yet fail to deliver consistent results. The gap is not a lack of intelligence. It is a lack of confidence in the underlying truth.

When data integrity is weak, insight becomes conditional. Leaders ask for extra validation. Teams cross-check figures. Decisions are revisited, refined, or delayed because the inputs never feel quite solid enough. The organisation moves forward, but with hesitation.

When data integrity is strong, the dynamic flips. Insight becomes actionable. Decisions are made with clarity and at pace because there is a shared understanding of what is actually happening. The organisation stops debating the numbers and starts acting on them.

This is the shift from insight to control.

Trust is not a soft cultural concept here. It is a hard performance condition.

Without it, even well-informed organisations struggle to act decisively. With it, execution becomes faster, more consistent, and more effective.

III.2 Commercial Impact

The effect of trust on performance is often underestimated because it does not appear as a single obvious lever.

It shows up across multiple areas simultaneously.

Forecasts become more reliable — not because they are more detailed, but because the underlying data is consistent. Variance drops, and when it does occur it can be understood and corrected quickly.

Organisations that move from fragmented to coherent data environments commonly see forecast accuracy improve by 10–20%, alongside measurable reductions in revenue leakage and decision latency.

Working capital stabilises. Decisions on inventory, pricing, and investment are based on a clearer view of demand and supply, reducing the need for buffers and contingencies.

Revenue performance becomes more predictable. Opportunities are better qualified, pricing aligns more closely to actual customer value, and the business can respond faster to market shifts.

Customer outcomes improve, often without any single visible transformation programme. Friction falls because the organisation is no longer working from disconnected customer views. Interactions become more consistent and issues surface earlier.

These effects are not independent. They all stem from one condition: decisions being made on a version of reality that actually holds together under pressure.

Independent research from MIT Sloan and Forrester links improvements in data integrity and governance to gains in forecast accuracy, operational efficiency, and revenue performance. Forrester's Total Economic Impact studies, in particular, show double-digit efficiency improvements when organisations move from fragmented to integrated data environments.

Where the underlying picture is coherent, performance follows.

III.3 Trust as Competitive Advantage

At a certain level of maturity, data integrity stops being merely an internal efficiency issue and becomes a genuine source of competitive advantage.

Organisations that operate on a coherent and reliable picture of reality move differently.

They make decisions faster because they are not constantly waiting for validation. They make fewer errors because the inputs are consistent. They execute more effectively because there is alignment not just in intent, but in understanding.

This combination creates momentum. Strategy turns into action with less friction. Operational plans hold together under pressure. Customer experience becomes more consistent because it is informed by a single view rather than multiple disconnected perspectives.

The performance difference is visible across sectors. Organisations with strong data integrity consistently outperform peers on execution speed, margin stability, and customer retention.

In these organisations, speed and confidence reinforce each other. Decisions are not just faster — they are more likely to be right.

This is where data integrity connects directly to execution frameworks such as SUCCESS. Without a stable understanding of reality, even well-defined strategies fail to deliver consistent outcomes.

By contrast, organisations operating on fragmented truth face a different reality. They move more cautiously, even when pressure is high. They revisit decisions not because conditions have changed, but because confidence in the inputs is low. Execution becomes uneven as different parts of the organisation interpret the same situation in conflicting ways.

Over time the gap widens. One organisation compounds advantage through consistent execution. The other absorbs friction through repeated adjustment and explanation.

The difference is not access to data. It is the ability to trust it.

Section III — Closing Position

By this stage, the relationship between data integrity and performance should be clear. Data does not drive performance on its own. Insight does not guarantee execution. Alignment, without a trusted picture of reality, does not hold under pressure. What connects all three is trust.

Not as an abstract idea, but as a practical condition that determines whether decisions can be made with confidence and acted upon consistently.

When that condition is met, organisations move with clarity and pace. Performance becomes more predictable — not because uncertainty disappears, but because it is understood within a stable frame of reference.

When it is not, the organisation compensates. It slows down. It validates. It revisits. It absorbs friction that does not need to exist.

This is the difference between organisations that generate insight and those that convert it into sustained results.

And it is why data integrity, at its core, is not a technical discipline. It is a performance capability — one that determines whether the organisation can turn understanding into action, and action into lasting advantage.

IV. The Only Stable Architecture for Truth

IV.1 Framing — Why Partial Solutions Fail

By this point the pattern is clear.

Organisations recognise the problem, see the performance and governance impact, and respond with investment. New platforms are introduced. Data models are redesigned. Integration layers are strengthened. In some cases entire transformation programmes are launched with the explicit goal of creating a “single source of truth.”

Yet despite the effort and spend, the underlying issue frequently remains.

The reason is straightforward: most responses are partial.

They address systems, processes, or data structures without tackling the conditions that allow distortion to persist — unclear ownership, distributed accountability, and contradictions that are managed rather than resolved.

As a result, organisations improve visibility without achieving real control. They end up with better reporting but not a more reliable picture of reality.

Research from Gartner and similar sources has shown that a significant proportion of data and analytics programmes fail to deliver the expected business outcomes. The common thread is not lack of technical capability. It is the absence of alignment between technology, ownership, and governance.

Stability requires something more deliberate — an architecture that defines how truth is owned, validated, and maintained across the organisation.

IV.2 The Oak A+B+C Architecture for Enterprise Truth

A stable architecture for truth rests on three interdependent components. Remove any one and the system becomes unstable.

A. Board-Level Reporting Line

Truth must be visible at the highest level — not as a collection of separate functional reports, but as a reconciled view of performance that leadership can actually rely on. This means bringing customer, commercial, and operational signals into a single coherent narrative rather than presenting them in parallel. Without this, fragmentation stays hidden. With it, inconsistencies become impossible to ignore.

B. Named Executive Accountability

Truth cannot be owned in the abstract. There must be a specific senior executive who carries clear accountability for the integrity of the organisation's operating reality. This is not technical ownership of data, but responsibility for how that data is interpreted, reconciled, and used in decision-making. The role needs real authority to challenge across functions and escalate when necessary. Without that authority, responsibility becomes symbolic. With it, contradictions can finally be surfaced and resolved.

C. Protected Capital Allocation

Maintaining integrity requires investment, but more importantly it requires protection from short-term trade-offs. Without a defined and protected allocation of capital and resource, integrity initiatives are routinely deprioritised in favour of immediate operational demands. Over time systems drift, processes diverge, and reliability erodes. Protected capital ensures integrity remains a core capability rather than an optional improvement.

These three components reinforce one another. The reporting line makes issues visible. Accountability ensures they are owned. Capital ensures they are addressed and sustained. Together they create the conditions under which a stable version of truth can exist.

IV.3 Governance First, Technology Second

Technology has an important enabling role, but it is not the starting point. In many organisations the sequence is reversed. Tools are selected and implemented first, with the expectation that governance will somehow follow. In practice it rarely does. Systems end up reflecting the same fragmentation that already exists — data is centralised but not reconciled, reporting becomes more comprehensive but not necessarily more trustworthy.

Effective architecture follows the opposite sequence. Governance is established first: ownership is defined, decision rights are clarified, and reconciliation processes are agreed. Only then does technology act as an enabler, supporting structures that are already in place. Capabilities such as master data management, data observability, and AI-driven analytics become far more powerful inside this framework because they operate within clear rules rather than in a vacuum.

IV.4 Failure Modes — How Architecture Breaks Down

Even with the best intentions, organisations often fall into predictable patterns that undermine stability:

- **Fragmented ownership**: Responsibility is spread across functions with no single point of accountability. Issues are identified but rarely resolved because no one has the mandate to enforce change.
- **Partial implementation**: Elements of the architecture are introduced in isolation — better reporting without clear accountability, or defined ownership without protected capital. Progress is made but does not hold.
- **Tool-led approaches**: Technology becomes the main focus while governance is treated as an afterthought. Sophisticated systems are delivered, yet the organisation continues to operate on inconsistent definitions and assumptions.
- **Short-term prioritisation**: Integrity work is repeatedly deprioritised in favour of immediate commercial or operational demands. Over time quality degrades and the organisation slips back into fragmented truth.

In every case the outcome is the same: the organisation never achieves a stable, trusted operating reality.

IV.5 Governance Equilibrium — A Practical Model

The interaction between governance and data integrity can be understood as an equilibrium.

At one end of the spectrum is **institutional integrity**: strong governance paired with high data integrity. Reporting is consistent, decisions are based on shared reality, and performance can be managed with confidence.

At the other end is **noise as normal**: fragmented data and weak governance. Inconsistency is accepted, decisions rely on interpretation, and control remains elusive.

Between these extremes sit two unstable states. One is **overbuilt and under-adopted** — heavy investment in systems and tools that are inconsistently used. The other is **heroic reconciliation** — individuals manually bridging gaps, carrying context in their heads, and keeping things moving through sheer effort.

Both can function for a while. Neither is sustainable.

The goal is to move deliberately toward institutional integrity, where governance and data integrity reinforce each other to create a reliable foundation for the business.

Section IV — Closing Position

At this stage the requirement is no longer simply to recognise the problem or understand its impact. It is to establish the conditions under which truth can be reliably maintained.

That requires more than better data and more than better tools. It requires an architecture that defines how truth is owned, validated, and sustained.

When that architecture is in place, data integrity becomes a managed capability rather than a recurring headache. Governance operates on solid ground and performance can be controlled with confidence.

When it is not, even sophisticated systems leave the organisation operating on fragmented reality.

This is the difference between organisations that invest in data and those that build a stable foundation for truth.

V. Implementation Roadmap — From Fragmented Truth to Controlled Reality

V.1 A 90-Day Control Reset

At this point the question is no longer whether data integrity matters. It is how quickly the organisation can bring it under control.

Many companies approach this as a full transformation programme — multi-year timelines, large-scale system changes, and ambitions to "fix all the data." The intent is understandable, but the approach often delays real impact. By the time results appear, the problems have already shifted.

A more effective route treats the challenge as a control reset rather than a transformation. The goal is not to perfect every piece of data. It is to establish a reliable operating reality that leadership can trust, govern, and act on — and to do it inside a defined window. This can be achieved in ninety days.

Phase 1 (0–30 Days): Establish Ownership and Visibility

Appoint a single accountable owner — or a tightly defined owning group — with a clear mandate to create a reconciled view of truth. This is a governance role, not a technical one. It carries authority to challenge across functions and escalate where necessary.

At the same time, make the current state visible. Use the Data Integrity Radar to assess accuracy, completeness, consistency, timeliness, and uniqueness across the key domains that matter commercially. The output is not another long report. It is a clear, shared picture of where integrity is strong and where it is breaking down — expressed in business terms leadership can act on.

Phase 2 (30–60 Days): Define the Truth Model

With visibility established, agree on the core definitions and measures that will underpin decision-making. Focus on what actually drives commercial outcomes: customer, revenue, pipeline, delivery performance, and the critical linkages between them.

Where multiple definitions exist, reconcile them. Where systems produce conflicting outputs for the same concept, establish which version will serve as the authoritative one for running the business. This does not require every system to be fully aligned immediately, but it does require clarity on what the organisation will treat as truth.

The Data Confidence Score becomes the simple, consolidated signal that tells leadership where decisions can be made with confidence and where further work is required.

Phase 3 (60–90 Days): Implement Governance Cadence

With ownership in place and a working truth model defined, embed governance into the organisation's operating rhythm. Introduce a regular cadence — aligned with existing financial and operational reviews — in which the reconciled view of reality is examined at the same level as performance numbers. Contradictions are no longer explained away; they are surfaced and resolved. This cadence mirrors the GROWTH framework rhythm: structured review, clear accountability, and prioritised action. The emphasis is on making integrity visible, acting on the highest-risk gaps, and building the habit of operating from a single trusted picture.

V.2 Measurement and Control

Sustained integrity requires measurement that actually drives behaviour. Traditional data-quality metrics — completeness percentages, error rates, reconciliation counts — are useful but too far removed from commercial outcomes. Shift the focus so integrity is judged by its real impact:

- Forecast accuracy as a proxy for data reliability
- Revenue and margin variance as signals of misaligned assumptions
- Customer churn and retention as indicators of how well the organisation truly understands its relationships

The Data Integrity Radar supports this by translating technical quality into a business-relevant view. Leadership can see not only where issues exist, but how they affect decision-making. This prevents "data theatre" — metrics tracked for their own sake — and keeps the focus on the organisation's ability to operate on reality that holds together.

V.3 Embedding Governance

Long-term success depends on more than processes. It requires the organisation to behave differently.

Incentives must reward shared outcomes rather than isolated functional performance. Reporting cycles must reinforce the reconciled view rather than allow parallel versions to persist. Most importantly, leadership behaviour sets the tone — particularly in how contradictions are handled. If discrepancies are rationalised or ignored, fragmentation returns quickly. If they are surfaced, challenged, and resolved, integrity strengthens.

Over time this stops being a project and becomes part of the operating model. Data integrity is no longer something the organisation *does*. It is how the organisation *runs*.

Section V — Closing Position

Moving from fragmented truth to controlled reality does not require a wholesale transformation. It requires a deliberate shift in focus: from improving data in isolation to establishing the conditions under which truth can be trusted and governed. The 90-day reset is not a complete solution. It is a starting point that creates ownership, visibility, agreed definitions, and a governance rhythm capable of being sustained. From there, improvement becomes continuous — driven not by programmes, but by the daily requirement to make decisions on a picture of reality that actually holds up under pressure. This is the difference between organisations that manage data and those that control performance.

VI. Scenario Stress Test — Understanding Exposure in Practice

VI.1 Distortion Sensitivity — Making the Invisible Visible

By this point the argument has moved beyond principle. If data integrity determines whether an organisation can trust the picture of reality it uses to make decisions, the next question is commercial: what could this actually be costing?

Distortion rarely arrives as one obvious failure. It builds quietly through small gaps that are easy to explain away — a forecast that keeps shifting, a customer segment that looks profitable until cost-to-serve is properly understood, a pricing model that hides leakage, or a delivery report that stays green while the customer experience deteriorates. None of these looks material in isolation. Together they create real exposure.

A scenario-based view helps leadership see the potential scale before it becomes a recognised loss.

Distortion Exposure by Annual Revenue

Illustrative exposure ranges at 3–5%, 5–7%, and 8–10%

Annual Revenue	3–5% Exposure	5–7% Exposure	8–10% Exposure
£500m	£15m–£25m	£25m–£35m	£40m–£50m
£1bn	£30m–£50m	£50m–£70m	£80m–£100m
£5bn	£150m–£250m	£250m–£350m	£400m–£500m

Illustrative modelling only — actual exposure depends on the organisation's operating environment and data integrity maturity.

Even conservative modelling points to a 5–10% performance drag at enterprise level across revenue leakage, margin erosion, working capital volatility, and time wasted reconciling rather than deciding. These figures should not be read as booked losses. They represent distortion exposure — the potential value at risk when decisions are made on fragmented or inconsistent information.

The range is deliberately cautious. Its purpose is not false precision but to force a simple leadership question: are we comfortable running the business without knowing where we sit on that spectrum?

VI.2 Vertical Application — How Exposure Shows Up

The exposure range is consistent at enterprise level, but how it manifests varies by sector and business model. Organisations often miss the problem because they look for data issues rather than commercial symptoms.

In SaaS and subscription models, distortion frequently appears early in the customer lifecycle. Sales conversion may look strong and onboarding may be reported as complete, yet early churn or poor adoption tells a different story. The customer has been "activated" internally, but value has not arrived quickly enough for them to stay.

In manufacturing and industrial environments, the tension usually sits between commercial commitments and operational reality. Sales works from one view of capacity, lead times, and priorities while production and supply chain work from another. The result is margin pressure, expediting costs, missed expectations, and a customer experience that feels less reliable than internal reports suggest.

In wholesale and distribution, distortion tends to hide in pricing, rebates, availability, fulfilment, and account hierarchies. Margins may look stable in aggregate while leakage builds quietly across transactions, customer groups, and channels. The customer experiences inconsistency; the organisation sees exceptions.

In professional and service-led organisations, the gap often appears between reported service performance and the customer's actual experience. SLAs are met, tickets are closed, and utilisation looks healthy, yet customers continue to chase, escalate, or quietly disengage.

These are not separate problems. They are sector-specific expressions of the same underlying condition: the organisation is running on a picture of reality that does not fully match what is actually happening.

VI.3 The Five-Driver Diagnostic

To move from broad concern to practical judgement, leadership needs a simple lens to assess exposure. The following five drivers provide that view. They do not require perfect data — only an honest look at how the organisation actually operates.

- **Identifier complexity**: How consistently are customers, products, accounts, contracts, sites, and transactions defined across systems? Simple and stable identifiers contain distortion. Complex, varying hierarchies and relationships allow duplication and misinterpretation to build quickly.
- **Revenue sensitivity**: How much does performance depend on accurate pricing, forecasting, segmentation, renewals, rebates, or usage data? In highly sensitive models, data issues move straight from administrative to commercial impact.
- **Incentive dependency**: Are teams rewarded on metrics that may not reflect full customer or commercial truth? When Marketing is measured on lead volume, Sales on closed deals, Delivery on SLA compliance, and Finance on margin protection, each function can act rationally while weakening the overall picture.
- **Cross-system fragmentation**: How many systems, spreadsheets, processes, and teams feed the organisation's view of performance? CRM, ERP, finance systems, service platforms, marketing automation, and local spreadsheets can each be useful individually but create a collective reality that requires constant interpretation.
- **Transaction density**: How frequently does the organisation create, update, price, deliver, amend, or renew customer activity? High-volume environments turn small issues into material ones through repetition. Lower-volume environments may have fewer incidents, but each carries greater complexity and value.

Together these drivers help leadership judge whether the organisation is likely sitting nearer the low, medium, or high end of the exposure range. They also challenge the easy assumption "we are probably fine." If identifier complexity is high, incentives are misaligned, systems are fragmented, and transaction density is significant, the burden of proof shifts. Assume exposure exists until you can demonstrate otherwise.

VI.4 Applying the Stress Test

The stress test is not meant to become another heavy modelling exercise. Its real value is in the leadership conversation it forces.

A practical discussion would ask:

1. Which revenue band are we operating in?
2. Which exposure range feels plausible given our five-driver profile?
3. Where would distortion appear first — revenue, margin, forecasting, operations, or customer experience?
4. What evidence do we have that current governance would actually detect and correct it?

The final question is the most important. Most organisations can tolerate some imperfection in their data. What they cannot afford is the inability to see where that imperfection is affecting decisions.

Used properly, the stress test turns data integrity from a background concern into a visible decision about exposure, confidence, ownership, and response. It feeds directly into the Data Integrity Radar and the 90-day control reset.

Section VI — Closing Position

A stress test is useful because it stops data integrity being abstract.

Once exposure is expressed in revenue, margin, decision speed, customer confidence, and governance control, it becomes much harder to leave in the background. The organisation can either continue operating on a broadly accepted but not fully trusted picture of reality, or it can quantify where the truth is weakest and bring that exposure under active control.

That is the shift this paper is asking leadership to make: from assumption to evidence, from interpretation to control, and from noise to trust.

VII. Board-Level Synthesis — From Insight to Decision

VII.1 What This Paper Actually Shows

Strip everything back and the point is simple. Most organisations cannot fully trust the picture of reality they are using to run the business. That is not because they lack data. In most cases they have more than enough. The real issue is how that data is pulled together, interpreted, and presented to leadership.

What looks like a coherent picture is often a stitched-together version of events. It holds just enough to support decisions, but not enough to stand up under pressure. That is where the gap sits — not between data and insight, but between what is reported and what is actually happening. Once that gap exists, everything that follows becomes harder to control.

VII.2 Why This Matters at Leadership Level

At an operational level, you can absorb this. Teams work around the inconsistencies. People sense-check numbers. Decisions get made with a degree of caution. It is not efficient, but the organisation still functions.

At leadership level that approach no longer works. You are making calls on capital allocation, growth strategy, risk, and customer direction. If the underlying picture is not reliable, neither are the decisions built on top of it.

This is the shift the paper is forcing. Data integrity is not a data problem. It is a control problem. If you cannot stand fully behind the numbers, you cannot claim to be in full control of the business.

VII.3 The Three Decisions You Can’t Avoid

Once you accept that reality, three uncomfortable but practical questions follow.

1. **Who actually owns the truth?** Not the CRM. Not Finance. Not “the business” in some vague sense. A specific person — or a very clearly defined small group — must own the reconciled view of reality. If no one does, multiple versions continue to co-exist. That may feel manageable day to day, but it collapses the moment you need a definitive call.
2. **How are contradictions handled?** Every organisation has them. Marketing says demand is strong. Sales says the quality is mixed. Delivery says expectations do not match reality. The question is not whether the differences exist. It is what happens to them. Do they get explained away? Or are they forced into a single version of truth that the whole organisation must work from? That is the difference between reporting and real governance.

3. **What level of uncertainty are you willing to run with?** Perfect data does not exist and never will. But unmanaged ambiguity is something else entirely. If you do not define what "good enough" looks like, decisions are always made on shifting ground. Some will land. Some will not. You will not always know why.

The Data Integrity Radar is useful here. It does not solve the problem on its own, but it makes the level of uncertainty visible and explicit. Most organisations never do that.

VII.4 What Actually Needs to Change

This is where many leaders expect a grand transformation plan — new systems, new teams, big programmes. That is not where this starts. It starts with control. Establish clear ownership. Make the gaps visible. Force reconciliation where it matters most. That is precisely what the 90-day control reset is designed to achieve. It will not fix every data issue, but it will fundamentally change how the organisation relates to its own operating reality. From there, improvement becomes ongoing rather than episodic.

VII.5 Where This Lands Strategically

Get this right and the business does not suddenly become perfect. But it does become clearer. Decisions move faster because you are not constantly second-guessing the inputs. Investment lands more effectively because it is based on something that actually holds up. Customer issues surface earlier because you are no longer relying on filtered or inconsistent signals.

Over time the advantage compounds — not in one dramatic leap, but through consistent, reliable execution. And that is usually where the real gap opens between organisations: not in strategy, but in how reliably they execute against it.

VII.6 The Only Question That Matters

At this point everything else is detail. The question is straightforward:

Can you trust the version of truth your organisation is using to run the business?

If the answer is yes, then this paper is simply confirmation. If the answer is no — or even "not entirely" — then this is no longer a data issue buried somewhere in the organisation. It is a leadership issue.

Until someone takes ownership of that truth and the organisation has a proper way of governing it, you are making decisions on ground that is not fully solid. Sooner or later, that shows up.

Closing Position

This is not about having better data. It is about knowing whether the picture you are working from is good enough to rely on. Once you see it that way, the question is no longer whether to act. It is how long you are comfortable operating without full control.

VIII. The Leadership Decision — Who Owns the Truth Now?

By this point the issue should no longer feel like a technical data concern. It is a leadership decision.

If the organisation cannot fully trust the picture of reality it uses to make decisions, the question is not whether the data team is busy enough, the CRM is properly configured, or the reporting pack looks professional. The real question is whether leadership has enough control over the truth the business is actually running on.

That question lands differently across the C-suite.

For the CEO

Data integrity determines whether the organisation is managing from a reliable operating reality. Strategy, growth, investment, and customer direction all depend on the quality of truth that reaches the top table.

For the CFO

It affects forecast confidence, capital allocation, margin visibility, and the credibility of performance reporting. If the numbers constantly need explaining, the issue is not only financial control — it is the reliability of the information feeding that control.

For the COO

It determines whether operational priorities are being set from what is actually happening, or from partial signals produced by disconnected systems, teams, and reporting routines.

For the CCO or CRO

It affects pipeline quality, customer value, retention risk, pricing confidence, and the ability to understand where growth is genuinely coming from.

For the CIO, CDO or technology leader

It reframes the challenge from connecting systems to enabling governed truth. Technology matters, but only when ownership, definitions, and decision rights are clear first.

For the board

It raises the central control question: can we demonstrate that the information used to run the business is reliable enough to support the decisions being made from it?

That is why data integrity cannot be left as a background improvement activity. It can be supported by technology teams, data specialists, and transformation programmes, but it cannot be fully delegated to them. The decision that matters sits with leadership.

- Who owns the reconciled version of reality?
- Where are contradictions resolved?
- What level of confidence is required before decisions are made?
- How is uncertainty made visible rather than quietly absorbed by the organisation?

Until those questions are answered, the organisation may improve data quality in pockets, but it will not control the truth it relies on. A business can have better dashboards, cleaner reports, and more sophisticated systems while still operating on fragmented reality.

Control only begins when leadership defines what truth means, who owns it, and how it is governed.

The practical next step is not another broad data transformation programme. It is a focused leadership review of where truth is trusted, where it is exposed, and where control needs to be established first.

Oak Consult's Data Integrity Radar provides that starting point. It assesses the reliability of the organisation's operating reality across accuracy, completeness, consistency, timeliness, and uniqueness, then translates that assessment into a business-relevant confidence view.

From there, a 90-day control reset can establish clear ownership of enterprise truth, visibility of the highest-risk distortion points, agreed definitions for the metrics that matter, and a governance cadence for resolving contradictions.

The aim is not to perfect the data. The aim is to give leadership a controlled, visible, and defensible foundation. The organisations that gain advantage will not be the ones with the most data. They will be the ones that can trust the truth they are using to make decisions.

If your organisation cannot answer that question with confidence, the next step is not to wait for a bigger system, a cleaner dashboard, or another transformation programme. The next step is to take ownership of the truth. Because once truth becomes governable, performance becomes controllable — and once performance becomes controllable, growth has a stronger foundation on which to scale.

Appendix A — Section Reference Tables (With Sources)

A.1 Section I — Truth, Noise and Economic Distortion

Source	Title	Relevance
MIT Sloan Management Review & BCG	*The Data-Driven Enterprise of 2025*	Shows link between data maturity and decision-making effectiveness
MIT Sloan Management Review	*Why Data Culture Matters*	Demonstrates how data trust impacts execution and performance
Forrester	*The Total Economic Impact™ of Data Governance*	Quantifies efficiency, cost reduction, and revenue benefits
Gartner	*Poor Data Quality Costs Organizations an Average of $12.9 Million a Year*	Establishes economic impact baseline of data quality issues
IBM	*The Cost of Poor Data Quality*	Widely cited benchmark for enterprise-level data quality cost

A.2 Section II — Governance Risk

Source	Title	Relevance
Financial Reporting Council (FRC)	*UK Corporate Governance Code (2018)*	Defines board responsibility for internal control and reporting integrity
Financial Conduct Authority (FCA)	*FG16/5: Guidance for firms outsourcing to the cloud*	Sets expectations for data governance and operational control
Bank for International Settlements (BCBS 239)	*Principles for Effective Risk Data Aggregation and Risk Reporting*	Global standard for data governance, aggregation, and reporting reliability
European Central Bank	*Guide on Effective Risk Data Aggregation*	Reinforces governance expectations for data accuracy and reporting consistency

A.3 Section III — Performance Impact

Source	Title	Relevance
MIT Sloan Management Review	*Becoming a Data-Driven Organisation*	Links data trust to decision-making speed and execution capability
Forrester	*Insights-Driven Businesses Set the Pace for Global Growth*	Shows performance advantage of organisations with strong data practices
McKinsey Global Institute	*The Data-Driven Enterprise of 2025*	Demonstrates productivity and performance gains from integrated data environments
Experian	*Global Data Management Research Report*	Provides evidence of data trust challenges and operational impact

A.4 Section IV — Architecture and Governance

Source	Title	Relevance
Gartner	*How to Build a Data and Analytics Strategy*	Highlights importance of governance and ownership over tools
DAMA International	*DAMA-DMBOK: Data Management Body of Knowledge*	Industry standard for structured data governance frameworks
Bank for International Settlements	*Supervisory Guidance on Risk Data Aggregation*	Reinforces need for board-level accountability and architecture
Harvard Business Review	*Data Governance Should Be Business-Led*	Supports governance-first, technology-second approach

---

A.5 Section V–VI — Implementation & Scenario Modelling

Source	Title	Relevance
Forrester	*Data Governance Maturity Model*	Supports phased implementation approach
McKinsey	*The Case for Digital Reinvention*	Links governance and data maturity to performance outcomes
PwC	*Data as a Strategic Asset*	Positions data as board-level strategic asset
KPMG	*Data Governance and Data Quality*	Practical governance and control frameworks